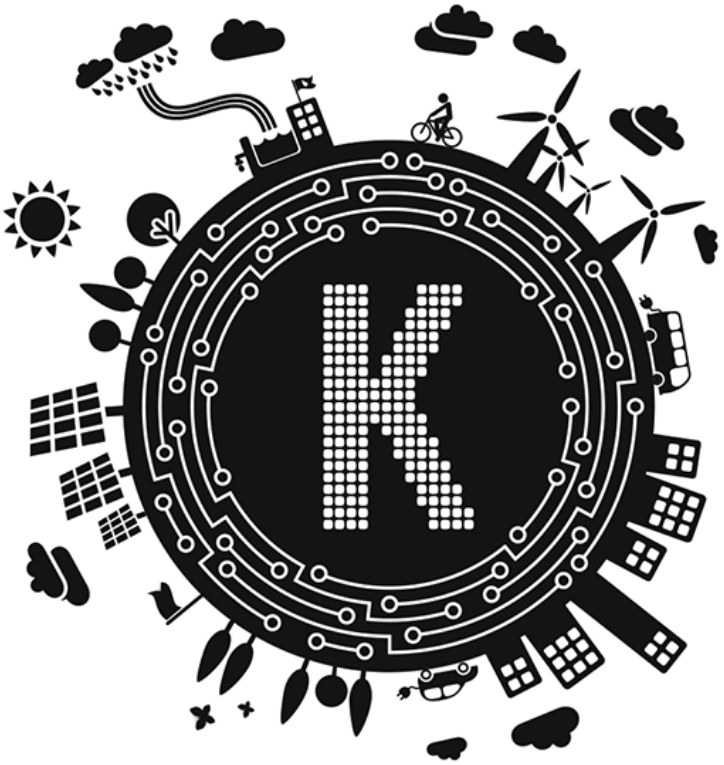
MICHAŁ ZAJDA

Kryptowaluty
dla zabieganych

MICHAŁ ZAJDA



Kryptowaluty
dla zabieganych

Tekst © Michał Zajda, 2022
Wszelkie prawa zastrzeżone

Redaktor prowadzący
Tomasz Brzozowski

Redakcja i korekta
Marek Stankiewicz, Agnieszka Al-Jawahiri, Anna Hadała-Żołnik

Projekt wnętrza i okładki, skład
Tomasz Brzozowski

Grafika na okładce
kula ziemska: radoma / depositphotos.com
ścieżki drukowane: Zybr78 / depositphotos.com

Konwersja do wersji elektronicznej
Aleksandra Pieńkosz

Copyright © for this edition
Insignis Media, Kraków 2022
Wszelkie prawa zastrzeżone

ISBN 978-83-67323-62-8

Insignis Media
ul. Lubicz 17D/21–22, 31-503 Kraków
tel. +48 (12) 636 01 90
biuro@insignis.pl, www.insignis.pl
facebook.com/Wydawnictwo.Insignis
twitter.com/insignis_media (@insignis_media)
instagram.com/insignis_media (@insignis_media)
tiktok.com/insignis_media (@insignis_media)

Książkę tę dedykuję moim dzieciom.
Mam nadzieję, że gdy dorośniecie,
spełnią się wszystkie optymistyczne scenariusze,
o których w niej piszę

Dokument chroniony elektronicznym znakiem wodnym

Zakupione w nexto: 3719581

Wstęp

O czym jest ta książka?

(Nie tak) dawno temu… czyli baśń o przyszłości

W 2009 roku pojawił się artykuł naukowy opisujący system pieniądza elektronicznego. Była to praca bardzo zgrabna, klarowna, napisana w stylu oksfordzkim; jej autor przyjął pseudonim Satoshi Nakamoto, ale do dziś nie wiadomo, kto się pod nim kryje. Artykuł opublikowany przez Nakamoto to osnowa systemu Bitcoin – najsłynniejszej kryptowaluty, o której słyszał chyba każdy.

Bitcoin – taki, jakim go dziś znamy i jakiego używamy – nie jest jednak dziełem wyłącznie Nakamoto. Pierwsze lata realizowania koncepcji anonimowego geniusza to praca nielicznego zespołu zapaleńców, którzy prowadzili wymianę myśli na dedykowanym Bitconowi forum. Pisali kod, dyskutowali, poprawiali. Przyświecał im wspólny cel. Mieli przeświadczenie, że „system” – czyli usankcjonowane funkcjonowanie społeczeństwa – nie jest w pełni sprawiedliwy. Nie wierzyli

w bezpieczeństwo swoich oszczędności w bankach. Nie ufali instytucjom. Wiele ich dyskusji inspirował *Manifest Cypherpunków* – sformułowany o wiele wcześniej niż praca Nakamoto i dotyczący samostanowienia i wolności.

Chyba już widzisz, dokąd to zmierza. Grupa hakerów chce stworzyć kod, który zapewni nienaruszalną prywatność, bezpieczeństwo i brak nadrzędnej instytucjonalnej kontroli w jednej z ważniejszych dziedzin życia: finansach. „Tak, tak… Słyszałem to chyba z tysiąc razy" – myślisz sobie pewnie. „Nuda". Otóż nie do końca…

Rysa na diamencie

Coś się wydarzyło. Doszło do zdumiewającego splotu okoliczności. Okazało się bowiem, że pomysły Satoshiego Nakamoto pojawiły się… o kilka lat za wcześnie! Kilka lat przed stworzeniem wydajnych komputerowych narzędzi, które byłyby w stanie zapewnić pełną anonimowość i prywatność. Hakerzy, o których wspomniałem, nie byli prorokami. Nie wiedzieli dokładnie, co przyniesie nam komputerowa przyszłość. I nie czekając na jej nadejście, stworzyli system, który nazywany jest pseudoanonimowym. Ta niedoskonałość – owa rysa na diamencie – i przemożna chęć używania nawet nieperfekcyjnego systemu, byle od zaraz, zmieniły nasz świat. To istny efekt motyla, który – jak widać dziś, po kilkunastu latach od pracy Nakamoto – wywołał prawdziwą lawinę. Lawinę pomysłów, nowych możliwości i zmian. Chciałbym cię zabrać w podróż po tym nowym świecie. To jeszcze nie jest nasz świat, lecz może sam przyspieszysz jego nadejście, kiedy przekonasz się, jaki tkwi w nim potencjał. Ale po kolei.

Kryptowaluty dla zabieganych

Zakładam, że sięgnąłeś po tę książkę, bo chcesz wreszcie zrozumieć, czym są kryptowaluty, ale nie planujesz poświęcać na to zbyt wiele czasu. Chcesz szybko poczuć się pewnie w świecie, który coraz bardziej przenika do twojej codzienności. Bo o kryptowalutach wszędzie jest głośno, a ty nie do końca wiesz, co odróżnia je od zwykłych pieniędzy. Słyszysz, że ktoś się na nich dorobił, a ktoś inny stracił. Że ten lub tamten sklep akceptuje płatność w kryptowalutach. Że doszło do jakichś kryptowalutowych skandalów lub plajt. Że nie warto się zajmować kryptowalutami. Albo wręcz przeciwnie, że kto nie wejdzie w świat kryptowalut już dziś, przegra życie. Jak odróżnić mity od faktów? Gdzie leży prawda? No i czym, do licha, tak naprawdę jest ten cały blockchain, który pojawia się prawie za każdym razem, kiedy mowa o bitcoinie i transakcjach elektronicznych? Na czym polega kopanie kryptowalut i o co chodzi z tymi obrazkami NFT?

Nie jestem zawodowym pisarzem. To po pierwsze. Po drugie: na co dzień obracam się w bardzo technicznym świecie kryptowalut, blockchainów i innych tego typu kwestii, rozmawiając z ludźmi, dla których wszystkie te technikalia to chleb powszedni. I postaram się te dwie moje cechy przekuć w zaletę: zrobię wszystko, by moja książka – podobnie jak artykuł Satoshiego Nakamoto – była zgrabna, klarowna i… możliwie krótka. No i dołożę wszelkich starań, by cię nie zanudzić, mimo że czasem będę opowiadał zwykłe historie, wzięte z codziennego życia. Postaraj się zwrócić uwagę na pewne niuanse, nowe nuty, które nie składają się w dobrze ci znaną melodię. Co usłyszysz? Dokąd cię zaprowadzą?

Dwa cele

Przyświecają mi dwa cele. Pierwszy to odejść od utartego myślenia o systemach kryptowalutowych i blockchainach jako systemach finansowych. To zjawiska o wiele większym znaczeniu! Chciałbym, żebyś dosłownie poczuł zew rewolucji wywołanej – między innymi – szczęśliwym zbiegiem okoliczności. Pisząc o kryptowalutach, nie sposób nie wspominać o pieniądzach, ale mam mocne postanowienie, by tę książkę tylko zacząć i zakończyć rozdziałami im poświęconymi.

Pieniądze są bardzo ważne. Ale nie wpłyną na nas, ludzi żyjących we w miarę bezpiecznym, w miarę nowoczesnym kraju zachodniej cywilizacji, tak bardzo, jak zupełnie nowe technologie, które powstały i powstaną dzięki kryptowalutom.

Drugi cel to przekazać ci wiedzę, która pozwoli ci krytycznie weryfikować dochodzące zewsząd informacje o kryptowalutach. „Bitcoin to nowy mesjasz!”, „Bitcoin to jawne oszustwo!”, „Kryptowaluty to narzędzie narkodilerów!”, „Bez bitcoina staniesz się niewolnikiem!”. Jako osoba specjalizująca się w tych technologiach powiem tak: tego typu wypowiedzi – padające zresztą z ust zarówno orędowników, jak i przeciwników kryptowalut – wydają mi się co najmniej przesadzone. Myślę o nich bardziej jako o sloganach wprowadzanych do informacyjnego obiegu przez gadające głowy, które brak swoich kompetencji ukrywają za kontrowersyjnymi, głośnymi hasłami. Żyjemy w świecie pełnym informacyjnego szumu i bez rzetelnej wiedzy łatwo się w tym wszystkim pogubić. Będę cały czas o tym pamiętał i postaram się wrócić do powyższych sloganów w kontekście, który pozwoli ci ocenić, czy tkwi w nich prawda, czy fałsz.

Odkryjmy przyszłość

Za chwilę razem przekroczymy portal prowadzący do fascynującego świata najnowocześniejszych technologii jutra. Tak! To głównie o nich będzie ta książka – pieniądze, finanse i ekonomia zejdą na dalszy plan. Owszem, dzięki lekturze *Kryptowalut dla zabieganych* pieniądz elektroniczny, który narodził się w głowie Satoshiego Nakamoto, odkryje przed tobą większość swoich tajemnic. Po przeczytaniu mojej książki dowiesz się jednak – mam nadzieję – o wiele więcej: jak technologie, które powstały niejako przy okazji tworzenia waluty przyszłości, mogą wpłynąć na przyszłość w ogóle, a nie tylko na przyszłość pieniądza. A zatem – idziemy!

1

Jak szybko zrozumieć kryptowaluty

Od walut do kryptowalut

Dlaczego tak trudno nam zrozumieć kryptowaluty? Bo myślimy o nich jak o jakichś magicznych nadpieniądzach, których potrafią używać wyłącznie ci, co posiedli tajemną, niedostępną dla przeciętnego śmiertelnika wiedzę. Odczarujmy ten świat. Zastanówmy się, czym jest zwykły pieniądz – na przykład polski złoty. W wyniku umowy społecznej, usankcjonowanej przez rząd, bank narodowy i inne banki, jest to środek wymiany handlowej. Pieniądzem mierzymy wartość towarów i usług, co pozwala na swobodny ich obrót: sprzedaż i nabywanie. Zwróć uwagę, że pojawiają się tu pojęcia umowy społecznej (jako społeczeństwo godzimy się na to, by przypisać monetom, banknotom i liczbom na naszych kontach bankowych określoną wartość nabywczą) oraz rządu i banków – gwarantów tejże umowy. Pieniądz to zjawisko, które intuicyjnie rozumieją nawet małe dzieci, choć one zapewne nie czują potrzeby, by ktoś – czyli w wypadku tradycyjnej waluty: rząd i banki – cokolwiek gwarantował.

A co by się stało, gdyby zmienić gwarantów umowy społecznej dotyczącej wartości pieniądza z rządu i banków – czyli instytucji „centralnych” – na jakichś innych? A może – skoro wartość pieniądza jest konsekwencją umowy społecznej – niech jej gwarantem będzie samo społeczeństwo, bez żadnych pośredników i instytucji. Te pomysły realizują właśnie pierwsze kryptowaluty. To pieniądz bez rządu i banków: ich miejsce zajął… blockchain.

Owad zatopiony w bursztynie

Czym jest ów tajemniczy blockchain? I dlaczego może zastąpić bank, czyli pełnić funkcję gwaranta naszej umowy społecznej co do wartości kryptowalut i ważności zawieranych nimi transakcji?

Blockchain to dosłownie łańcuch bloków. Stanowi sposób organizacji pierwszych kryptowalut, na przykład słynnego bitcoina. Zanim jednak zaczniesz myśleć o blockchainie jako o blokach połączonych w łańcuch, wyobraź go sobie inaczej.

Nick Szabo, wpływowa postać w świecie kryptowalut i specjalista w dziedzinie kryptografii komputerowej (kryptografia to nauka zajmująca się zabezpieczaniem informacji przed niepowołanym dostępem – teraz już wiesz, skąd cząstka „krypto” w słowie „kryptowaluty”), porównał łańcuch bloków do skamieniałego owada zatopionego w wielkim bursztynie (coś takiego nazywa się fachowo inkluzją). Taki owad sprzed milionów lat reprezentuje transakcje, a narastający (przy założeniu, że obok jest źródło żywicy) wokół niego bursztyn – warstwę zabezpieczającą. Im więcej lat upłynie, tym większy stanie się bursztyn, a owad – jeszcze lepiej zabezpieczony. Nie dostaniesz się do niego inaczej, jak tylko przez

poważne uszkodzenie bursztynu, a wszelkie próby naruszenia skamieniałej żywicy będą wyraźnie widoczne.

Podobnie jest z blokami dołączanymi na końcu łańcucha. Blok niczym pojemnik przechowuje naszą transakcję, a kolejne przyłączane do łańcucha bloki (z kolejnymi zapisanymi w nich transakcjami) – w analogii do kolejnych warstw żywicy pokrywającej owada zatopionego w bursztynie – skutecznie uniemożliwiają zmianę historii i treści transakcji. Teraz już chyba widzisz, dlaczego blockchain jest wymarzonym narzędziem, które samo z siebie – przez taki, a nie inny zapis kryptowalutowych transakcji – zapewnia ich bezpieczeństwo na lata. Blockchain robi to, co w wypadku zwykłych pieniędzy należy do obowiązków banku.

Niejednemu rozwiązaniu blockchain na imię

Blockchain dziś to ogólne określenie systemu organizacji kryptowalut, mimo że rozmaite rozwiązania mogą zupełnie odbiegać od klasycznego wyobrażenia łańcucha bloków. Czasem blockchain to tak zwane przeplatanki, odwrócone bloki czy sieci pojedynczych operacji. Niewykluczone, że sam twórca Bitcoina* inspirował się strukturą baz danych, która niekiedy ma postać uszeregowanych bloków.

Dlaczego dziś odchodzimy od tej „klasycznej” wersji? Cofnijmy się o jakieś czterdzieści lat. Być może już tego nie pamiętasz, ale to był czas kaset wideo. Tak oglądało się filmy – magnetowid VHS, telewizor wielkości komody i kopia piątej kopii *Rambo*. Obiekt pożądania każdego fana kina! A dziś? Dziś mamy Netflix i inne serwisy streamingowe. Podobnie zmienił się blockchain, z tą różnicą, że tempo ulepszeń w tej

dziedzinie jest znacznie większe niż w wypadku dystrybucji i konsumpcji treści wideo.

W czym współczesne blockchainy są lepsze od tego „klasycznego”? Wróćmy do przykładu zestawiającego współczesne serwisy streamingowe z kasetą VHS. W przeciwieństwie do kasety, na której mieści się określona, skończona i wiadoma zawartość, streaming polega na dostarczaniu na nasze urządzenia małych cząstek filmu, które w miarę oglądania tworzą jego całość. Tak jest łatwiej, taniej i szybciej; mamy też nieporównywalnie większy wybór i dostępność od ręki. Esencja postępu. Mniej więcej tak samo wypada porównanie pierwszych systemów blockchainowych z tymi stosowanymi obecnie.

Blockchain to zupełnie nowa gałąź przemysłu. I w dużej mierze tego określenia można używać wymiennie ze słowem „kryptowaluta”. Jest nawet lepsze – podkreśla bowiem technologiczne, a nie finansowe pochodzenie tej nowej, fascynującej idei, która może zmienić nasz świat.

Kryptowaluty, blockchain – jeden czort?

Czy blockchain to w stu procentach to samo, co kryptowaluta? Nie. Jest tu pewien niuans, który chciałbym omówić. Satoshi Nakamoto w swojej pracy nigdzie nie użył słowa „kryptowaluta”. Aby opisać system tworzący pieniądz elektroniczny, stosował słowo „moneta” (*coin*). Tym sposobem z popkultury blockchainowej wyłoniła się idea kryptowaluty.

Monety w blockchainie to część jego mechanizmu. Jego krwiobieg. Transportują, koordynują, wynagradzają. Jeśli ten „życiodajny” nośnik blockchaina – moneta – stanie się produktem i przedmiotem handlu, to mówienie o nim „kryptowaluta” jest już bliższe prawdy. Gdy jednak

pozostanie tylko wewnętrznym nośnikiem, a produktem jest cała platforma, prawdę bardziej odda myślenie o takim systemie jako o blockchainie.

Tego typu niuanse sprawiają, że czasem trudno – nawet informatykom – pojąć ideę kryptowalut. Mam jednak nadzieję, że na razie większość tego, co przeczytałeś, nie nastręczyła ci większych problemów. Owad w bursztynie. Łańcuch bloków. Monety. Pamiętaj o tych analogiach i idziemy dalej!

Dlaczego zwykli informatycy czasem nie rozumieją kryptowalut?

Informatycy nie rozumieją kryptowalut? Czy to nie oni stworzyli blockchain?

Wspomniałem o tym już we wstępie. Początkowo – w roku 2009 i kolejnych latach – kryptowalutami zajmowali się ludzie, którzy nie należeli do orędowników mainstreamowych rozwiązań finansowych. Ich działalność przypadła na okres gwałtownego rozwoju „tradycyjnych" technologii informatycznych: każdego dnia pojawiał się wówczas nowy komunikator, nowa gra na Facebooku czy nowy filtr do zdjęć i filmów w serwisach społecznościowych. Tak wyglądał informatyczny mainstream. A Bitcoin tworzyli hobbyści – ludzie bardzo inteligentni, ale często niepodążający z głównym nurtem rozwoju technologii, stymulowanym przez wielkie koncerny i ich produkty. Naukowcy, kryptolodzy. Z lekką przesadą można by określić ich mianem wyrzutków lub… cyberpunków! Rozwiązywali podobne problemy, co reszta „zwykłych" informatyków, ale w odosobnieniu, niezależnie. No i przede wszystkim mieli bardzo ważną

misję, której cel w dużej mierze wykluczał czerpanie z publikowanych, dostępnych powszechnie rozwiązań.

Co było tym celem? Decentralizacja. To dość intuicyjne pojęcie. Przeciwieństwo centralizacji.

Większość poważnych instytucji jest bardzo scentralizowana. Można to potraktować jako pewien anachronizm, bo z historycznego punktu widzenia centralizacja była metodą zapewnienia bezpieczeństwa. Centralna jednostka, władza bądź instytucja jest z definicji dość zamknięta i trudno dostępna. Pozostaje pod ścisłą kontrolą prawną. Jeśli kiedyś chciałeś otworzyć bank, musiałeś dysponować budynkiem z grubymi murami, kratami i innymi fizycznymi zabezpieczeniami. Bank ma wiele przywilejów i z reguły jest bardzo dochodowy. Jego prowadzenie obliguje jednak do pilnowania porządku i przestrzegania zasad. System bankowy ma też wady. Jest korupcjogenny. I bardzo złożony, gdyż wymaga coraz bardziej złożonego prawa, zabezpieczającego go przed możliwymi nadużyciami, w tym nielegalnym przepływem informacji.

Zwolennicy decentralizacji są orędownikami zupełnie przeciwnej koncepcji. Zaprojektowali system, który zapewnia bezpieczeństwo, obchodząc się bez centralnej władzy i jej regulacji. Dostępny dla wszystkich algorytm stoi na straży porządku, a kto nie stosuje algorytmu, nie może być częścią systemu. Jest to rozwiązanie o wiele prostsze od centralnych, w dodatku otwarte dla każdego.

No dobrze, ale jak taki otwarty system w ogóle może działać, skoro każdy może w nim… robić, co tylko chce? Otóż kryptowaluty w swoim DNA mają – oprócz decentralizacji – jeszcze jedną bardzo ważną cechę. Jest nią zasada braku zaufania. Ponieważ w całym systemie nie istnieje żadna centralna władza ani jakakolwiek inna jednostka, której możemy ufać, jedno z naczelnych założeń musi być właśnie takie. Te dwie cechy

systemu – decentralizacja i brak zaufania – wywracają wszystko do góry nogami. To właśnie dzięki temu systemy blockchainowe, a nie skostniałe tradycyjne rozwiązania, promują innowacje.

I tu dochodzimy do zagadki braku zrozumienia kryptowalut przez informatyków tradycjonalistów. Większość z nich tworzy swoje systemy w sposób scentralizowany, nawet gdy działają one na tysiącach rozproszonych komputerów. Użytkownicy tych systemów, na przykład czatów, pokładają zaufanie w korporacjach, wierząc, że ich dane, zdjęcia czy filmy nie będą nadużywane, a treść prywatnych rozmów jest znana tylko ich uczestnikom.

Kryptowaluty w swój mentalny wzorzec mają wdrukowane coś skrajnie przeciwnego. Nie pozwalają obserwować się czujnemu oku policjanta, chcą jednak zapewnić użytkownikom bezpieczeństwo i wolność. Jak to pogodzić? Wierz mi – da się!

I jeszcze taka analogia: wyobraź sobie średniowieczne miasteczko z rynkiem i odchodzącymi od niego uliczkami. To model centralny – w nim wszystko, co ważne, dzieje się na rynku: to tam prowadzą wszystkie drogi w mieście. Tymczasem model zdecentralizowany bardziej przypomina Wenecję – miasto z wieloma niezależnymi wyspami, czyli niezależnymi ośrodkami handlu (a więc historyczne przykłady sprawdzają się w nowoczesności!). Teraz trzeba sobie zadać pytania: jak zapewnić bezpieczeństwo w miasteczku z rynkiem, a jak w „rozproszonej” Wenecji? Gdzie jest łatwiej zadbać o to bezpieczeństwo? Które z miast jest bardziej odporne na atak? W którym z nich katastrofa naturalna w mniejszym stopniu zaszkodzi jego funkcjonowaniu? Dalsza lektura tej książki przyniesie odpowiedzi na te pytania, choć podejrzewam, że już je znasz!

Kryptowaluty? Ja wolę BLIK-a!

Dlaczego przeciętny zjadacz chleba w naszej części świata zwykle dość obojętnie przechodzi obok wynalazku kryptowalut? Sam pewnie zastanawiasz się, i to nawet już po tym wszystkim, co do tej pory przeczytałeś: „Po co mi te śmieszne internetowe pieniądze? Szczególnie że mogę puścić dowolny przelew w kilka sekund, a ekspresowej płatności dokonam BLIK-iem. A jeśli nie znam konta odbiorcy, to należną kwotę szybko prześlę na jego numer telefonu… Szybko i bezpiecznie. Oprócz tego jest całe mnóstwo innych sposobów płatności: PayPal, Apple Pay, Google Pay – nic, tylko przelewać, mimo banków, centralizacji i tego wszystkiego, w czym niby mają być lepsze kryptowaluty”.

William Gibson, jeden z moich ulubionych pisarzy science fiction (i twórca cyberpunka), stwierdził kiedyś: „Przyszłość jest już dziś, tylko nierówno rozłożona”. I może trudno ci będzie w to uwierzyć, ale Polska w tym konkretnym przypadku jest jednym z miejsc, gdzie przyszłość jest dziś. Dzięki temu, że nasz system bankowy zaczął powstawać na przełomie lat osiemdziesiątych i dziewięćdziesiątych poprzedniego wieku, mamy niemalże najnowszą infrastrukturę na świecie… I to ona pozwala się nam cieszyć tak wygodnymi, zróżnicowanymi, bezpiecznymi i szybkimi transferami pieniężnymi.

Nie tak daleko od nas, w Wielkiej Brytanii, jeszcze kilka lat temu przelew dochodził do odbiorcy przez niemal tydzień! Podobnie było w Stanach Zjednoczonych. Niby dwa ośrodki innowacji, a tymczasem ich obywatele musieli po imprezie rozliczać się przez tydzień! To nie wszystko: w Stanach do tej pory w większości banków trzeba wypełnić papierowy formularz, by dokonać przelewu międzynarodowego. Ta kuriozalna sytuacja spowodowała rozwój aplikacji finansowych, takich jak PayPal czy

Revolut. Stoją za nimi prywatne firmy, często start-upy, które są scentralizowane i czerpią w pełni z zalet tego systemu, ale już niekoniecznie w stu procentach potrafią strzec naszych finansów. Jest to tak duża część usług, że ma własną nazwę: FinTech (*Financial Technologies*), choć my blockchainiarze wolimy nazywać je TradFi (*Traditional Finance*). Słabość gwarancji finansowych sektora FinTech z pewnością przyczyniła się do rozwoju blockchaina.

Pójdźmy jednak dalej. Wbrew temu, jakie odnosisz wrażenie, tylko niewielka część ludzi na świecie ma dostęp do banków, a już z pewnością niewielu może korzystać z aplikacji na smartfonach. A mimo to społeczności składające się z takich osób całkiem nieźle sobie radzą! Budują swoje ekonomie amatorskimi środkami. Przykładem niech będzie ekonomia impulsów telefonicznych oparta na tanich telefonach na kartę prepaid – z tego rozwiązania korzystali ludzie bez dostępu do zaawansowanych technologii, w Afryce i Azji.

W naszym codziennym życiu na razie nie odczuwamy zalet zdecentralizowanej kryptowaluty. Nasz system finansowy jest stabilny na tyle, że nie musimy zgłębiać tajników polityki monetarnej. Nie myśl jednak, że tak będzie zawsze. Mieszkańcy Turcji po kryzysie 2021 roku czy właściciele firm na Cyprze, których zawartość kont bankowych została okrojona do okrągłych stu tysięcy euro, coś o tym wiedzą…

Dżungla pomysłów

Rozumiem twoją obojętność na kryptowaluty. I to być może z niej wynikała u ciebie nieznajomość tematu. Po co masz rozumieć coś, z czego i tak nie zamierzasz skorzystać? Zwykłe pieniądze są w porządku. Wystarczają.

Przelewy szybko dochodzą. Środki na kontach raczej są bezpieczne. Kryptowaluty? Po co to komu?

Dlatego mam wielki plan. Najpierw – ale tylko dla porządku – przedstawię ci zalety używania kryptowalut jako zdecentralizowanego środka płatności. Może przyznasz mi trochę racji. Postaram się, by dalsze części książki dotyczyły tematyki finansów w jak najmniejszym stopniu – bo ileż można?!

Chciałbym za to zabrać cię na wyprawę przez istną dżunglę pomysłów, które wyrosły w blockchainowym świecie. To tak, jakbyśmy zaczęli rozmawiać o różnych środkach transportu. Samochodach, motocyklach, statkach i samolotach. Przemierzają w różny sposób różne środowiska – lądy, oceany, przestworza. Maszyny te łączy silnik, któremu zawdzięczają napęd. Blockchain dla systemów zdecentralizowanych jest takim właśnie silnikiem. Rozumiem, że jazda samochodem już ci się znudziła… To może masz chęć na spływ łodzią po Amazonce?

---

* Tu małe wyjaśnienie formalne. Nazwa „Bitcoin” (a także „Ethereum” itp.) jako nazwa protokołu, systemu lub blockchaina zapisywana jest od wielkiej litery, natomiast jako nazwa waluty – zupełnie jak „złoty” – od małej; granica znaczeniowa bywa jednak płynna (przyp. red.).

2

Jeszcze trochę o pieniądzu

– O co chodzi z tymi całymi kryptowalutami?

– To elektroniczne pieniądze. Wymyślił je w 2009 roku gość o pseudonimie Satoshi Nakamoto i jego pomysł się przyjął.

– No dobra, ale co w nich odkrywczego w porównaniu ze zwykłymi pieniędzmi na koncie w banku?

– Na przykład to, że nie ma tam banków.

– Więc kto pilnuje interesu?

– To właśnie ta najbardziej odkrywcza część. Wyobraź sobie, że masz elektroniczne monety zapisane na komputerze albo jeszcze lepiej gdzieś w chmurze. Gdyby można je było kopiować jak pliki, byłyby bezwartościowe. Satoshi Nakamoto wymyślił cały system, który zapewnia wartość i bezpieczeństwo elektronicznych monet i zawieranych nimi transakcji. Ten system nazywa się „blockchain". Nakamoto wykorzystał go do stworzenia pierwszej kryptowaluty: bitcoina.

– A tak, bitcoin. Gdzieś słyszałem, że jeden bitcoin to setki tysięcy złotych. Kogo na to stać?

– W przeciwieństwie do euro czy złotego, które dzielą się na części setne, czyli centy i grosze, bitcoin dzieli się aż do osiemnastego miejsca po przecinku! Jeden bitcoin ma o wiele więcej cząstek niż kilogram mąki. Nie zawsze jednak był taki drogi. Wiesz, że jest coś takiego jak Bitcoin Pizza Day? To upamiętnienie 22 maja 2010 roku, kiedy to jeden z pierwszych użytkowników bitcoina kupił dwie pizze za dziesięć tysięcy bitcoinów. Dziś to około czterdziestu milionów dolarów. Nie dość, że od

tamtych czasów wzrósł kurs bitcoina, znacznie wzrosły też opłaty za dokonywane nim przelewy.

– Płatne przelewy?! Bez sensu! Czy ktoś naprawdę używa kryptowalut?!

– Bitcoin stał się drogi, ale jest też stabilny. Używamy go do innych celów niż płacenie za kawę. To pierwsza, ale tylko jedna z wielu kryptowalut. Wymyślony przez Satoshiego Nakamoto blockchain – mechanizm Bitcoina – od początku wykorzystywany jest przez programistów do tworzenia nowych kryptowalut. Jedne z nich są szybkie, inne – tanie. Każda z nich ma swoje optymalne zastosowanie, a zastosowań kryptowalut jest bardzo wiele.

– To może poczekać jeszcze kilka lat, aż ktoś stworzy idealną kryptowalutę do wszystkiego?

– Idealna powszechna kryptowaluta może nigdy nie powstać… Warto zatem już teraz wsiąść do tego rozpędzającego się pociągu. Zresztą chyba wiem, jak cię do tego zachęcić, a jednocześnie nie przytłoczyć wszystkimi możliwościami. Opowiem ci o dwóch najważniejszych i niezależnych od siebie projektach: Bitcoinie i Ethereum. Mimo że były jednymi z pierwszych, bardzo możliwe, że wyznaczają początek i koniec tego, co da się zrobić z kryptowalutami. Bitcoin to taki prosty komputer, który potrafi dodawać i odejmować. Działa podobnie jak bank, który dodaje i odejmuje pieniądze na naszych kontach. Ethereum zaś to uniwersalny komputer, potrafi prawie wszystko to, co zwykły laptop. Wiele projektów realizowanych przez ethereum nie jest nawet związana z pieniędzmi. Na ethereum można by nawet zagrać w grę wideo… choć byłoby to dość kosztowne i powolne. To właśnie ethereum jest narzędziem, za pomocą którego najłatwiej wypróbować nowy pomysł na kryptowalutę. Sam więc widzisz, że dziesiątki tysięcy kryptowalut mieści się gdzieś pomiędzy bitcoinem a ethereum. Ich projektów jest tak dużo, bo każdy twórca chce wprowadzić swoje mniej lub bardziej sztywne zasady działania. Każdą z nich napędza jednak podobny co do podstawowej koncepcji działania silnik: blockchain. To on gwarantuje wartość i bezpieczeństwo elektronicznego pieniądza.

– A jakie są twoje ulubione kryptowaluty?

– O, mam ich bardzo dużo. Z zainteresowaniem obserwuję te, które służą do ochrony danych medycznych. Gram w kilka kryptowalutowych gier, bo w blockchainie punkty zdobyte w grze stają się prawdziwą walutą. Zastanawiam się, czy nie zainwestować w jakiegoś motoryzacyjnego klasyka… Jest wiele projektów, które ułatwiają i zabezpieczają takie szczególne transakcje. Wiesz, że interesuję się

polityką. Tu też sprawdziłby się blockchain – mógłby przyspieszyć i uprościć głosowanie, eliminując jednocześnie wszelkie nadużycia. Skończyłby się wreszcie ten cały bałagan przy organizowaniu i przeprowadzaniu wyborów. Sam widzisz: kryptowaluty, a raczej mechanizmy i technologie, jakie za nimi stoją, dają wprost nieskończone możliwości. Ciekawe, jak to się wszystko rozwinie…

– Nadal nie jestem przekonany, ale teraz naprawdę mnie zaskoczyłeś! Muszę się dowiedzieć trochę więcej o tym blockchainie, który najwyraźniej wszystkim rządzi…

Pieniądze to technologia

Kolejne generacje waluty, która jest namacalnym wcieleniem pieniędzy, stają się coraz bardziej abstrakcyjne. Samo pojęcie pieniądza można rozumieć jako umowę społeczną. Waluta i jej transfer to wyraz tej umowy. Tysiące lat temu walutą mogła być koza. Lub jabłka. Nie tak szybko odeszliśmy od waluty bazującej na towarach, ale nawet w jej ramach dokonywał się postęp. Pszenica stanowiła bardziej pożądaną walutę niż ziemniaki czy koza. Nie psuła się, nie można było jej ukryć przed poborcą podatkowym i bardzo łatwo się dzieliła na potrzebne nam w danej sytuacji porcje. Opisuje to James C. Scott w swojej doskonałej książce *Jak udomowiono człowieka*. Podobnie sól. Nie dość, że miała swoją wartość jako produkt, była też łatwa w podziale i w transporcie oraz powszechnie uznawano ją za dobro.

Historycznie pieniądze reprezentowało coś trudnego do wytworzenia lub coś, co było dostępne w ograniczonym stopniu. Taki przedmiot stanowił nośnik wartości, a w dodatku można było go przemieścić, przetransferować. Pieniądz okazał się kluczem do odblokowania ewolucji małych plemion w wielkie społeczności składające się z wyspecjalizowanych podgrup. Takie podgrupy nie były samowystarczalne. Ktoś produkował buty, a ktoś inny mleko. Handel

wymienny (wymiana dóbr), co oczywiste, był możliwy tylko w bardzo ograniczonym zakresie i, jak łatwo sobie wyobrazić, nastręczał mnóstwo kłopotów. Pieniądz rozwiązał ekonomiczny problem przypadkowości potrzeb. W złożonym społeczeństwie handel wymienny był hamulcem rozwoju. Przypadkowi ludzie mają konkretne potrzeby. Szewc nie zawsze potrzebuje mleka, a mleczarz nowych butów. Zanim odnajdą wspólną walutę – medium pośredniczące – stracą dużo czasu i energii. Pieniądz reprezentowany przez poręczny, unikatowy, odporny na zniszczenie przedmiot pozwolił mleczarzowi i szewcowi dokonywać transferu wartości w czasie i w przestrzeni. Ów wartościowy przedmiot stał się uniwersalną wyceną ich pracy – wymiernym przelicznikiem jej wartości. Pozwolił zamieniać tę pracę na spełnianie własnych potrzeb.

Następnym etapem ewolucji pieniądza były metale szlachetne, które skierowały postęp ku utrzymywaniu wartości i unikatowości. Pieniądz był nie tylko coraz łatwiejszy do przeniesienia w przestrzeni, ale także w czasie. Magazynował wartość w uniwersalnej formie. Nośniki waluty stały się odporne na pogodę i o wiele mniejsze. Ciekawym aspektem metali szlachetnych jest ich samozawieralność. Sztabkę złota możemy zważyć i od razu wiemy, ile jest warta. Sztabka złota zawiera w sobie wartość.

Potem nadeszła era papieru. Pojawiły się banknoty, obligacje i inne papiery wartościowe. Waluta i pieniądz potrzebują gwaranta, który odpowiada za ich wartość. To główna różnica między pieniądzem papierowym a bazującym na metalu szlachetnym. Czy warto zaryzykować i zaufać gwarantowi w zamian za łatwość korzystania z pieniądza? Oczywiście. Pieniądze papierowe stały się jeszcze łatwiej podzielne. Jeszcze lżejsze i prostsze w wymianie. Pieniądz zaczął cyrkulować szybciej niż kiedykolwiek wcześniej. A szybki obrót pieniądza napędza gospodarkę i jest źródłem dobrobytu.

Erę papieru od ery prądu, a następnie komputerów, dzieliło już naprawdę niewiele czasu. Właściwie to tutaj zmiana była najmniejsza. Sprawdzony już system przenieśliśmy w świat bitów i internetu. Kluczowym czynnikiem zawsze był gwarant, strażnik – bank – który doglądał prawidłowego przetwarzania transakcji i pilnował zdeponowanych w nim środków. Pieniądze nie mogą powstawać w niekontrolowany sposób. Chciałoby się rzec: pieniądze nie mogą brać się z powietrza… ale to stwierdzenie nie do końca oddaje rzeczywistość; to temat na oddzielną książkę.

Czy ewolucja pieniądza dobiegła już końca? Nie opanowaliśmy przecież, przynajmniej na razie, kolejnej technologii komunikacyjnej po manipulowaniu elektronami w układach scalonych i fotonami w światłowodach… Ale mimo to, mimo braku wyraźnego technologicznego skoku, ewolucja pieniądza wciąż postępuje.

I to właśnie kryptowaluty są jej owocem.

Kryptowaluty – nowa jakość elektronicznej wymiany informacji

Czym w takim razie są kryptowaluty? Czy są to pieniądze? Skąd się biorą? Ile ich jest? Musimy „rozbroić” groźne pojęcie kryptowalut krok po kroku, by się przekonać, że wcale nie jest aż takie groźne.

Przede wszystkim nie traktujmy kryptowalut jako jednolitej koncepcji. Jest bardzo wiele kryptowalut. Przypomina to trochę sytuację rodem z Dzikiego Zachodu, kiedy istniało wiele prywatnych banków. Emitowały swoje prywatne waluty, których używali okoliczni mieszkańcy. Obecnie działa wiele firm tworzących kryptowaluty. Tylko jedna z tych kryptowalut

jest szczególna. Bitcoin – był pierwszy i nie stoi za nim żadna firma; nawet jego twórca pozostaje jak dotąd nieznany.

Ale czym jest kryptowaluta?

Czy jest pieniądzem?

Kryptowaluta jest elektroniczną jednostką wymiany wartości między ludźmi. Jej wartość pochodzi wyłącznie z docenienia przez rynek jej nienaruszalności. Podobnie jak trudno było podrobić złotą monetę i jak trudno jest podrobić nowoczesny banknot, tak trudno jest podrobić kryptomonetę.

Wynika z tego, że kryptowaluta dość dobrze odtwarza cechy klasycznego pieniądza. Czy poza łatwością transferu oferuje coś jeszcze?

Kryptowaluty są bardzo dobrze podzielne: większość z nich dzieli się z dokładnością do kilkunastu miejsc po przecinku (co oznacza, że jeden kryptowalutowy grosik to na przykład jedna trylionowa, czyli 0,000000000000000001 wyjściowej jednostki monetarnej). Kryptowaluty bardzo łatwo przechować. Można do tego wykorzystać pamięć masową zwykłego komputera, pendrive lub wyspecjalizowany portfel kryptowalutowy. Rdzeniem kryptowalut jest kryptografia – dla przypomnienia: nauka zajmująca się zabezpieczaniem informacji przed niepowołanym dostępem – co sprawia, że tych elektronicznych pieniędzy po prostu nie da się podrobić.

I tak dochodzimy do kluczowej różnicy między kryptowalutą a tradycyjnym pieniądzem. Kryptowaluty nie potrzebują strażnika, gwaranta, banku, by można było prowadzić ich wymianę, czyli dokonywać nimi transakcji. Kryptowaluty nie potrzebują również banku, który przechowywałby środki w formie fizycznej i elektronicznej. Obecnie by dysponować gotówką, musisz wypłacić papierową wersję pieniędzy z bankomatu, czyli de facto z banku. Przed fizyczną wypłatą twoje

pieniądze przechowywał, a więc poniekąd kontrolował, bank. W przypadku kryptowalut mamy pod pełną osobistą kontrolą elektroniczną i zarazem jedyną wersję pieniądza. Paradoksalnie dzięki temu kryptowaluta – byt wirtualny – zyskuje swego rodzaju fizyczność.

Ta fizyczność elektronicznego pieniądza została doceniona przez użytkowników. Docenił ją rynek i stąd wzięła się jego wartość. Stało się to w okresie podkopanego zaufania do banków komercyjnych i centralnych, kreatywnej polityki monetarnej wielu państw i niepokojących kryzysów finansowych. Ten splot wydarzeń motywował twórców do budowy systemów kryptowalutowych – nie potrzebują one centralnego strażnika, gwaranta, by pieniądz w ich krwiobiegu miał fizyczną wartość, a jednocześnie oferują wszystkie wygody korzystania z elektronicznych finansów.

Niektórzy twierdzą, że pierwsza kryptowaluta, bitcoin, to najbardziej zaawansowana forma pieniądza. Jest odporny na inflację – docelowo będzie tylko 21 milionów bitcoinów. Jest niepodrabialny i możemy operować jego ułamkowymi częściami. Bazuje na mechanizmie blockchaina, umożliwiającym globalny transfer środków między użytkownikami systemu. Wszystkie te cechy wynikają z niego samego i nikt nie potrzebuje żadnej instytucji – żadnego gwaranta i strażnika – żeby wszelkie reguły operacji finansowych były dochowywane przez cały czas.

Skąd wziąć kryptowalutę?

Kryptowaluty kupujemy u brokerów na giełdach kryptowalutowych. To odpowiednik giełd papierów wartościowych. Różnica jest taka, że zamiast oferować akcje spółek, giełdy kryptowalutowe podłączyły swoje komputery

do sieci kryptowalutowych i oferują monety kryptowalut. Monety te można przekazywać w ramach jednej sieci.

Aby kupić kryptowalutę, przelewamy tradycyjne pieniądze na swoje konto u brokera, a następnie w jego portalu wymieniamy na kryptowalutę. W odróżnieniu od tradycyjnych giełd możemy teraz przenieść nasze kryptowalutowe monety do osobistego portfela kryptowalutowego, który jest poza zasięgiem giełdy, brokera czy państwa. Od tej chwili do przelewów do portfeli innych użytkowników danej kryptowaluty potrzebujemy tylko programu portfela i internetu. Wszystko to odbywa się już teraz bez pośrednictwa banku czy brokera – kryptowalutą płacimy jak najzwyklejszą gotówką na targu.

Czy kryptowaluty zastąpią tradycyjne pieniądze?

Analitycy i obserwatorzy ekonomiczni wciąż pytają z przekąsem: kiedy dojdzie do powszechnej adopcji kryptowalut, skoro są ponoć takie wspaniałe? Kiedy kryptowaluty zburzą dotychczasowy ład? Kiedy stwierdzimy, że nie potrzebujemy już strażników i gwarantów, czyli banków? Kiedy naszą pensję zamiast na nasze konto bankowe otrzymamy prosto do kryptowalutowego portfela?

Nigdy. Ale ponieważ nigdy nie należy mówić „nigdy”, powiem tak: na pewno nie w najbliższym czasie. Bo nie ma czegoś takiego jak uniwersalna kryptowaluta.

Jest wiele prywatnych i publicznych kryptowalut. Każda ma swoją niszę. Każda jest wewnętrzną jednostką systemów informatycznych nowej generacji zwanych blockchainami.

Niektóre z kryptowalut są bardzo stabilne i powszechnie uchodzą za bezpieczne. Inne są wątpliwej jakości i proweniencji. Jeszcze innymi płaci się wyłącznie za usługi firm, które je stworzyły właśnie w tym celu.

By w tym niezwykle różnorodnym świecie wymiana wartości przebiegała szybko i sprawnie, powstają rozmaite systemy wspomagające. Zdecentralizowane giełdy, monitory aktywności i wycen, protokoły inwestycyjne i pożyczkowe. Cały ten ekonomiczny ekosystem nazywany jest DeFi – to skrót od pojęcia *Decentralized Finance* oznaczającego finanse zdecentralizowane.

DeFi to bardzo młody ekosystem. Czasem powiela znane z tradycyjnej ekonomii instytucje w nowym wirtualnym świecie – świecie bez strażników i gwarantów. Czasem tworzy zupełnie nowe produkty. Wspólnym mianownikiem jest jednak demokratyzacja zdecentralizowanych sieci. To ich użytkownicy tworzą płynność. To oni dostarczają kapitał do pożyczek innym użytkownikom. Nic nie dzieje tutaj się za zamkniętymi drzwiami banków inwestycyjnych.

Potęga blockchaina, wrażliwość kryptowalut

Kryptowaluty to krwiobieg blockchaina, a jednocześnie produkt, który pretenduje do bycia pieniądzem. Przez to, że blockchain to zupełnie nowa koncepcja zrealizowana w ramach nowych, rewolucyjnych systemów, kryptowaluty aspirujące do funkcji pieniądza są na razie dość podatne na spekulacje i ataki. To nic nowego – odbicie działań człowieka w domenie tradycyjnych finansów, w których od czasu do czasu zdarzają się przecież nadużycia i oszustwa. Każdy, kto chce zarobić na wahaniach kursów kryptowalut, podejmuje spore ryzyko. Póki co jesteśmy świadkami

wczesnego etapu powstawania świata kryptowalutowej ekonomii. Potrzebujemy edukacji i dalszego rozwoju systemów pomocniczych, by ów świat stał się w pełni bezpieczny i przyjazny.

Chciałbym jednak zakończyć dyskusję o kryptowalutach jako pieniądzu, źródle szybkich fortun i sensacji na rynkach. Uważam za to, że teraz jest idealny moment, by poznać bliżej silnik napędzający kryptowaluty, czyli blockchain; kryptowaluty są tylko jednym z wielu produktów wywodzących się z blockchaina, podobnie jak na przykład komunikator jest jednym z wielu programów, których można używać na komputerze.

Dlaczego blockchain jest taki ważny? I dlaczego uważam, że ten uniwersalny wynalazek zmieni losy internetu i świata wirtualnego, do którego powoli się ze wszystkim przenosimy? Dlatego, że za jego pomocą da się rozwiązać wiele problemów, z którymi obecnie mierzymy się w naszej internetowej egzystencji.

Główną zaletą blockchaina jest zaufanie, o które – paradoksalnie – w tym systemie nie trzeba specjalnie się starać. Pamiętasz analogię ze skamieniałym owadem uwięzionym w bursztynie, którego zabezpieczają kolejne warstwy zastygającej żywicy? Albo dosłowne wyobrażenie łańcucha bloków, w którym każdy dołączany blok to zapis kolejnej transakcji? W jednej i drugiej analogii przyrost (bursztynu, łańcucha) stanowi samoistne zabezpieczenie wszystkiego, co działo się wcześniej.

Blockchain to rozproszona baza danych, która nie wymaga zaufania od partnerów, z którymi chcemy współpracować. Ludzie, firmy i komputery mogą wymieniać się w nim dobrami i informacjami bez banków i pośredników.

W języku angielskim istnieje określenie *settlement platform*, jego polski odpowiednik to „platforma rozliczeniowo-transakcyjna”. Samo słowo

settlement – porozumienie, umowa, ugoda, rozliczenie – to podstawowe pojęcie finansowe, ostatni krok zatwierdzający transakcję kupna/sprzedaży. Ryneczek z warzywami to też *settlement platform*. Podobnie jak nowoczesne systemy giełdowe, choć tam nie kładzie się nacisku na akt zgody obu stron co do warunków transakcji. Bo *settlement* to umowa, z której zawarcia obie strony mają być zadowolone.

Systemy blockchain są właśnie takimi platformami umowy, platformami zgody. Są narzędziem do ogólniejszej organizacji naszego życia, wykraczającej poza aspekt finansowy, który jest obecnie obsługiwany przez systemy giełdowe.

Blockchain – przyszłość internetu

Blockchain jest kolejnym krokiem ewolucji użyteczności internetu. Internet u swojego zarania zapewniał tylko (choć to „tylko” to i tak bardzo dużo!) natychmiastowy dostęp do zgromadzonych online danych i dzielenie się nimi. Następnie umożliwił nam komunikację. Komunikacja i dane to budulec kolejnego etapu ewolucji: tworzenia społeczności. Media społecznościowe zdefiniowały drugą dekadę XXI wieku. Kryptowaluty są narzędziem do przejścia w kolejne stadium – tworzenia pełnoprawnej wirtualnej ekonomii. Jest to coś zupełnie innego niż stosowanie terminali kart płatniczych i przelewów online do przenoszenia naszych pieniędzy między fizycznymi bankami. Wirtualna ekonomia to stworzenie przepływu pełnowartościowej waluty w warstwie wirtualnej, bez odwoływania się do fizycznego świata: banków, terminali, dokumentów. Wirtualna waluta to dopełnienie wirtualnych towarów; działa w tej samej domenie.

Wszystko to nie byłoby możliwe, gdyby nie blockchain. W kolejnych rozdziałach przeczytasz, co jeszcze potrafi to wspaniałe narzędzie. Zamierzam cię zaskoczyć!

3

Przelewanie i kopanie

Jan obudził się dopiero w późnej porze śniadaniowej. Co za weekend, tyle się wydarzyło…

„Czy ja oddałem Kasi pieniądze za kawę po squashu? Ups… Ale niedawno wygenerowała dla mnie adres swojego portfela… Mam… Przelane”.

Adres portfela

To właśnie między innymi po to powstał bitcoin. By przyjść z pomocą w sytuacjach podobnych do tej z powyższego przykładu. Został pomyślany jako system pieniądza elektronicznego. Dziś jednak mamy BLIK-a, PayPala, przelewy na numer telefonu i jeszcze inne metody błyskawicznego transferu środków. Gdzie tu jakakolwiek różnica?

Poszukajmy jej! Kasia wygenerowała dla Jana specjalny, unikatowy adres. Numer konta, tylko pewnie trochę dłuższy i z literami – pomyślisz. Otóż nie! Konta posiadamy jako klienci banków. Zdarza się, że dysponujemy kilkoma kontami i mamy kilka numerów kont. Rejestrujmy je w urzędzie skarbowym, czasem używamy ich do automatycznego opłacania

rachunków za telefon i wpłacania darowizn na szczytne cele. Numer konta zamieszczamy w umowach z kontrahentami, zleceniodawcami czy pracodawcami celem otrzymania należności za naszą pracę, usługi lub sprzedaż jakichś dóbr. I ten sam, tak ważny przecież numer musimy udostępnić koledze od piłki nożnej, jeśli chcemy, by przelał nam pieniądze za przekąskę zjedzoną w przerwie meczu.

Stwarza to duże pole do nadużyć. Znanym z mediów przykładem, że coś może pójść nie tak, jest Jeremy Clarkson, który buńczucznie obwieścił, że każdy może poznać numer jego konta i nic nikomu z tej wiedzy nie przyjdzie. „Można mi tylko przelać kasę. W drugą stronę to nie zadziała” – stwierdził. Trochę się zdziwił, gdy później na wyciągu zobaczył, że pobrano mu środki z konta, zupełnie bez jego wiedzy. W związku z tym, że znalazły się one na koncie fundacji charytatywnej, wszystko odbyło się zgodnie z prawem i bez naruszenia protokołów bezpieczeństwa. Można sobie jednak wyobrazić, że protokoły te „nagną” nieuczciwi pracownicy banków, albo że pojawi się w nich luka spowodowana błędem w oprogramowaniu!

I na tym tle wyraźnie rysuje się przewaga kryptowalut. Stworzenie odpowiednika numeru konta – czyli tego adresu, który Janowi przekazała Kasia – jest bardzo tanie i możliwe bez pośredników. Wszystko to dzięki dynamicznie rozwijającej się kryptografii (nauce o… dobra, już się nie będę powtarzał). Taki adres generujemy w programie zwanym portfelem. Zwykle możemy dodać przy adresie opis, dla kogo i w jakim celu stworzyliśmy takie… „subkonto” (posłużyłem się tu analogią bankową). Jednocześnie wszystkie wygenerowane w naszym portfelu adresy są „dziećmi” jednego „rodzica”: adresu głównego. Teraz jednak muszę znów powiedzieć ci kilka słów o kryptografii. To ważne, bo w ten sposób lepiej wszystko zrozumiesz.

Co zabezpiecza adresy kryptowalutowe?

Pamiętasz może historie o szpiegach ze starych powieści? Poufną informację szyfrowali jakimś tajnym hasłem. Używali trudnych do odgadnięcia kluczy. Szyfr Cezara sprzed dwóch tysięcy lat polegał na podmianie każdej litery wiadomości na inną, oddaloną od danej o cztery miejsca w alfabecie. Przy dzisiejszej mocy obliczeniowej komputerów takie szyfry w ogóle nie zapewniają bezpieczeństwa. Jednak nawet gdyby były wystarczająco złożone i dzięki temu trudne do złamania, i tak miałyby bardzo dużą wadę. Żeby dwie strony mogły się skomunikować, musiały wymienić się wspólnym sekretem – musiały przekazać sobie ten właśnie klucz. Wystarczyło wtedy je podsłuchać i cała zaszyfrowana wiedza stawała się jawna. Czy da się jednak zaszyfrować wiadomość tak, by druga strona mogła ją odczytać bez żadnej wcześniejszej komunikacji? I tu wkracza kryptografia… z lat dziewięćdziesiątych ubiegłego wieku. Choć… nie do końca: w rzeczywistości metody asymetrycznego szyfrowania, o których chcę tu napisać, pochodzą jeszcze z lat siedemdziesiątych. Pozwalają na zaszyfrowanie wiadomości i odczytanie jej wyłącznie przez odpowiedniego odbiorcę bez konieczności przesłania mu wcześniej tajnego hasła! Brzmi nieprawdopodobnie? Tak też uważali kryptolodzy, ale kiedy w końcu odkryli, jak to zrobić, od razu zdali sobie sprawę z wagi swojego wynalazku. Wszystkie prace o kryptografii asymetrycznej utajniono. Urządzenia szyfrujące objęto ścisłą kontrolą eksportową, surowszą niż w przypadku broni, w szczególności w USA. Kryptografia stała się dziedziną bezpieczeństwa narodowego. Dopiero w połowie lat dziewięćdziesiątych, wraz z niezależnym i otwartym rozwojem kryptografii, wiedza ta stała się jawna. Obecnie korzystamy z kolejnej generacji kryptografii „z nowym silnikiem” – są nim tak zwane krzywe

eliptyczne. Te krzywe to bardzo ciekawy twór matematyczny. Już nieraz przydały się ludzkości. To między innymi dzięki krzywym eliptycznym i ich własnościom Andrew Wiles zdołał przeprowadzić słynny dowód wielkiego twierdzenia Fermata w 1994 roku. Obecnie krzywe eliptyczne – rzecz jasna inne i inaczej niż w dowodzie wielkiego twierdzenia Fermata – z powodzeniem stosuje się w kryptografii. Ale nie wchodźmy w szczegóły, wystarczy wiedzieć, że dzięki specyficznym krzywym eliptycznym kryptografia asymetryczna jest bezpieczniejsza, szybsza i tańsza. Jej zasada jednak pozostała w gruncie rzeczy taka sama.

Poznajmy ją zatem!

Opiera się ona na dwóch kluczach: prywatnym i publicznym. Działając w trzewiach naszego oprogramowania (szyfrując i dekodując informacje), są praktycznie niewidoczne dla użytkownika. Jak więc wyglądają te klucze? Możesz myśleć o nich jak o hasłach, których używamy na co dzień, tyle że te potrafią mieć po kilka tysięcy znaków! (Przyjmuje się, że na stronie A4 standardowo mieści się 1800 znaków ze spacjami, więc… dobrze, że nie trzeba tych kluczy wpisywać!)

I teraz tak: klucz publiczny staje się naszym adresem. A nasz adres to taka skrzynka na listy. Każdy może coś do niej wrzucić, ale tylko właściciel z kluczem prywatnym może coś z niej wyjąć. Tak to wygląda po stronie odbiorcy.

Wysłanie środków z innej skrzynki jest analogiczną operacją, również wymagającą klucza prywatnego, bo przecież też otwieramy skrzynkę (w tym wypadku swoją) i przekazujemy jej zawartość w kolejne miejsce.

Klucz prywatny jest zatem tym, co musimy bezwzględnie chronić. To potwierdzenie naszej tożsamości i zabezpieczenie własności. Klucze mają swoją hierarchię, dzięki której musimy pilnie strzec tylko kluczy-„rodziców” (to adresy naszego portfela). Najlepiej zapisywać je w tak

zwanych portfelach sprzętowych – urządzeniach na pierwszy rzut oka przypominających pendrive’y, wyposażonych jednak w wiele usprawnień, które zabezpieczają nasze tajemnice przed niepożądanym dostępem. Klucze-„dzieci” (czyli adresy „subkont” portfela) mogą być albo jednorazowe, albo można przechowywać je w mniej bezpiecznych lokalizacjach (jak przeglądarka internetowa czy telefon). Postaram się do kwestii bezpieczeństwa wracać jak najczęściej.

Transakcja

Jan przelał środki do portfela Kasi. W tradycyjnych systemach finansowych określamy to słowem „transakcja”. Pewnie już zdążyłeś się przyzwyczaić, że w blockchainie wszystko dzieje się trochę inaczej. Tak jest i tym razem. Okazuje się bowiem, że słowo „transakcja” pochodzi z terminologii baz danych, czyli specjalistycznego oprogramowania do wydajnego przechowywania i organizowania informacji.

Gdy chcemy dokonać zmiany zawartości bazy, używamy w tym celu transakcji, czyli tak zwanej operacji niepodzielnej. Wyobraź sobie komentarze pod postem na Facebooku. Aby były uporządkowane zgodnie z chronologią napływania, musimy skończyć jeden zapis (sfinalizować transakcję) i dopiero po tym pozwolić kolejnym użytkownikom dodać swoje przemyślenia.

Co by się działo, gdyby nie było transakcji? Gdybyśmy z konta, na którym jest 15 złotych, chcieli pobrać dwa razy po 10 złotych, nie korzystając z operacji transakcji, mogłoby się to udać! Mogłoby się zdarzyć tak, że serwer banku w tej samej chwili otrzymałby dwa zapytania o przelew 10 złotych; za każdym razem uznałby, że stan konta wynosi

15 złotych i udzieliłby pozwolenia na wykonanie przelewu. Na koniec dnia bilans wykazałby pięciozłotowe manko! Dlatego wszystkie poważne systemy używają transakcji. Zapytania są uszeregowane i procedowanie kolejnego może zacząć się dopiero wtedy, gdy skończy się obsługa poprzedniego. W naszym przykładzie po pierwszej wypłacie z konta zostanie na nim 5 złotych i kolejna wypłata 10 złotych nie dojdzie do skutku.

Chyba nie uwierzysz, kiedy ci powiem, że jeszcze do niedawna nawet wielkie banki miały w systemach sporo dziur w tym zakresie.

W blockchainie słowo „transakcja” wraca do swojego pierwotnego informatycznego znaczenia: to znaczy każda operacja kryptowalutowa jest transakcją, ale nie zawsze taka operacja jest związana z transferem gotówki! Transakcja to modyfikacja zawartości bazy danych, którą jest blockchain.

Jak przebiega transakcja bankowa

W dużym uproszczeniu: w banku każde nasze konto ma rubryczkę z zapisem ilości środków. Transakcja bankowa to usunięcie z rubryczki nadawcy stanu bieżących środków, wpisanie do niej nowej niższej wartości, następnie usunięcie stanu środków z rubryczki odbiorcy i wpisanie do niej wartości powiększonej o przelaną kwotę. Zauważ, że to bank realizuje akt przelania środków na konto odbiorcy: usuwanie i zapisywanie. Realizując przelew, w rzeczywistości nie przelewamy środków, lecz udzielamy bankowi zgody na pomniejszenie i powiększenie stanu odpowiednich kont. Bank jest centralnym strażnikiem i gwarantem, by wszystko odbyło się prawidłowo. Wszyscy musimy mu ufać.

Jak przebiega transakcja kryptowalutowa

Transakcja kryptowalutowa jest czymś zupełnie innym. Pod adresem, który zabezpieczamy osobistym kluczem prywatnym, znajduje się portfel, a w nim prawdziwe środki! Transakcja kryptowalutowa polega na sporządzeniu następującej wiadomości: „z adresu *xyz* przelewam środki na adres *uvw*”. Podpis kryptograficzny nadaje autentyczność i chroni nienaruszalność tej wiadomości. Jest ona rozgłaszana po całej sieci klientów blockchainowych. I na tym właśnie polega istota blockchaina: to sieć, która rozumie nasze wiadomości, czyli transakcje! Każdy uczestnik sieci zanim zaksięguje zmiany na zawsze, sprawdzi, czy są możliwe do wykonania. Czy adres *xyz* posiada wystarczające środki? Tak! Wtedy transakcja staje się częścią wspominanego już wcześniej bloku, czyli pudełka, które ją przechowuje. Nie ma żadnego strażnika, gwaranta. Nikomu nie musimy ufać, bo nie ma takiej potrzeby. Każdy uczestnik tej sieci prowadzi własną księgowość. Dzięki nowoczesnej kryptografii jest to wbrew pozorom bardzo proste!

Zwróć uwagę na kolejną zaletę kryptografii. W treści naszej wiadomości są tylko dwa adresy: *xyz* oraz *uvw*. Usłyszał ją każdy uczestnik sieci. Tak więc system jest w pełni jawny: wszyscy wiedzą, że doszło do transakcji pomiędzy dwiema stronami. Nikt jednak nie wie, kim one są: wiadomość ani słowem nie wspomina ani o Janie, ani o Kasi. Oznacza to, że system jest pseudoanonimowy. Po zatwierdzeniu transakcji tylko Kasia będzie mogła użyć środków spod adresu *uvw*, gdyż tylko ona dysponuje otwierającym tę „skrzynkę” kluczem prywatnym. Kasia nie musi być online. Przelane na adres jej portfela środki pozostaną w nim na zawsze lub do momentu, kiedy zdecyduje się je przenieść. Nikomu nie musi mówić, że adres *uvw* należy do niej.

Czy to wszystko jest bezpieczne? O tak, i to bardzo. Trudno tu dokonać jakiegokolwiek oszustwa. Powiem więcej: podatny na oszustwa jest sposób działania tradycyjnych banków. Niepodejrzewającym niczego złego klientom banków oszust może podstawić stronę podszywającą się pod stronę banku – wyglądającą na pierwszy rzut oka identycznie jak oryginał. Za jej pośrednictwem oszust może przechwycić dane (login i hasło) chroniące środki zgromadzone na naszym koncie. Dzięki temu zyskuje nad nimi kontrolę i może nimi dysponować w dowolny sposób, zanim się zorientujemy! A kiedy się zorientujemy, nasze konto może być już puste… W zdecentralizowanym świecie takie niebezpieczeństwo nie istnieje. Transakcja wysłana w niepowołane ręce nie jest groźna, bo nie można zmienić jej treści. Chęć wykonania przelewu nigdy nie sprawi, że przekażemy komuś dane do naszego portfela (nie ma tu konieczności logowania na stronie banku, podawania loginu i hasła itd.). I jeśli nawet wyślemy przelew do oszusta zamiast do właściwego odbiorcy, ten niczego więcej – oprócz odebrania przelewu – nie będzie mógł zrobić. Transakcja w blockchainie nie jest udzieleniem pozwolenia zmiany stanu naszego konta, tylko dokładną instrukcją, miniprogramem, co zrobić z naszymi środkami: „Przelej 10 złotych z adresu *xyz* na adres *uvw*”. Treści takiej wiadomości oszust nie będzie mógł zmienić na przykład na: „Przelej wszystkie środki z adresu *xyz* na adres *uvw*”. Za nienaruszalność treści wiadomości transakcyjnej odpowiada silna kryptografia.

Musisz pamiętać tylko o jednym: nie możesz, nie możesz, nie możesz pod żadnym pozorem przekazywać nikomu danych swojego portfela! To coś absolutnie prywatnego!

Blok

Wspomniałem o bloku. To ten blok, który jest w nazwie „blockchain”. Blok to po prostu ułatwienie, pudełko lub pojemnik. Bloki przechowują transakcje i stosujemy je w celu przetworzenia większej liczby transakcji jednocześnie. Pojedyncza transakcja to coś mikroskopijnego w stosunku do możliwości obliczeniowych sieci i komputerów XXI wieku. Pierwsze blockchainy, w tym bitcoinowy, dla ułatwienia i optymalizacji wydajności organizowały transakcje w bloki. Zupełnie jak listonosz, który nie dowozi każdego listu osobno, tylko wypełnia dostawczaka pod sufit i przewozi większą liczbę przesyłek. Tym sposobem cała nowa gałąź przemysłu informatycznego zyskała nazwę wywodzącą się z rdzenia jednego z jej najstarszych produktów.

Podsumujmy zatem naszą wiedzę, uzupełniając ją o pojęcie bloku: przelew kryptowalutowy polega na utworzeniu transakcji (wiadomości skąd, dokąd i ile przekazać) i wpuszczeniu jej do sieci. Każdy węzeł sieci sprawdza, czy transakcja jest poprawna, i zaksięguje ją u siebie, czyli zmodyfikuje treść swojej bazy danych. Te operacje przeprowadzane są w większych turach – blokach. Pojedyncze transakcje są bowiem zbyt małe, by księgować je osobno. W pierwszych systemach blockchainowych księgowanie trwało parę minut, w obecnych zajmuje nie więcej niż kilkanaście sekund.

Łańcuch

Skąd w nazwie „blockchain” słowo *chain* – łańcuch?

Bloki, jak już wiemy, są jednostką organizacji danych. Kiedy blok wypełni się transakcjami – zupełnie jak dostawczak listonosza przesyłkami – jest rozgłaszany w sieci. Napotykamy tu problem praktyczny.

Zastanówmy się nad taką sytuacją. Jan przesyła pieniądze Kasi, po czym Kasia zasila adres Lilii. Pozornie wszystko gra. Sieć jest bardzo szybka, w końcu sygnały w światłowodach biegną z prędkością światła. Kasia, widząc w swoim portfelu dziesięciozłotowy przelew od Jana, przesyła 8 złotych Lilii. Pierwsza transakcja to „*xyz* (Jan) 10 zł *uvw* (Kasia)”, druga to „*uvw* (Kasia) 8 zł *abc* (Lilia)”. Obie transakcje teoretycznie są poprawne, gdyż w portfelu Kasi w chwili wysłania środków do Lilii było 10 złotych. Ten stan rzeczy istniał w pewnym miejscu i czasie z punktu widzenia jednego z obserwatorów w sieci – Kasi. Zobaczyła, że otrzymała przelew i część kwoty postanowiła przekazać dalej. W czym problem?

Blockchain to gęsta sieć połączeń. Jej węzły przekazują transakcje z prędkością światła. Może się jednak zdarzyć, że informacja o przelewie do Lilii przybędzie na jakiś odległy węzeł, zanim trafi do niego transakcja między Janem a Kasią. Ze względu na mapę połączeń sieci i skończoną prędkość przekazywania informacji wiadomości o tych dwóch operacjach zamienią się kolejnością. Jest to możliwe, bo w dane miejsce sieci dwie transakcje mogą przybyć dwiema różnymi drogami. Różnymi połączeniami i przez różne serwery. Ta różnorodność dróg jest podstawą odporności internetu na lokalne awarie. Jest też jednak źródłem rozmaitych opóźnień.

Wróćmy teraz do Kasi i Lilii. Gdy transakcje zamienią się kolejnością, nie będą już poprawne. Przed przelewem od Jana portfel Kasi był pusty! Transakcja między Kasią a Lilią, wykorzystująca środki przelane uprzednio przez Jana, zostanie odrzucona, więc blok wypełniany transakcjami do zaksięgowania nie będzie zawierał przelewu do Lilii. Oczywiście żadne pieniądze nie zginęły, bo skoro nie doszło do przelewu do Lilii, nie pomniejszyła się zawartość portfela Kasi. Chcę jednak tym prostym przykładem zwrócić twoją uwagę na fakt, że odlegli użytkownicy sieci

mogą mieć inny obraz prawdy, czyli tego, co się wydarzyło. I wszyscy mają rację! Po prostu ze względu na skończoną prędkość rozchodzenia się informacji każdy ma trochę inny ogląd rzeczywistości. I tu przechodzimy do serca każdego systemu kryptowalutowego.

Gdy blok wypełni się transakcjami, węzły sieci zaczynają pracę nad jego zaksięgowaniem. Wielkość bloku jest z góry ustalona, podobnie jak waga torebki cukru w każdym sklepie. Bloki, które nie są jeszcze zaksięgowane, mogą się różnić. Różnią się kolejnością transakcji, mogą zawierać nawet różne transakcje (na przykład w kilku z nich może brakować informacji o przelewie Kasi do Lilii). Jak zatem wybrać taki blok, który będzie źródłem prawdy dla wszystkich użytkowników kryptowaluty?

Uff, robi się gęsto. Musimy zrobić małe podsumowanie: każda transakcja kryptowalutowa jest rozgłaszana po całej sieci. Każdy pełnoprawny użytkownik sieci sprawdza, czy jest poprawna. Jeśli tak, podaje ją dalej.

A teraz zjedźmy pod ziemię… do kopalni i górników!

Górnicy, konsensus, funkcja hashująca

Kluczową rolę w zaprowadzeniu porządku w systemie odgrywają górnicy (*miners*). Górnicy pracują w szczególnych węzłach sieci. Ich zadaniem jest wybranie jednej wersji prawdy, która zostanie uznana przez wszystkich bez żadnych zastrzeżeń. Każdy może być górnikiem. Wystarczy skorzystać z górniczej wersji oprogramowania do kryptowalut, nasłuchiwać bieżących transakcji i pracować nad zatwierdzeniem nowego bloku. Zatwierdzenie bloku to zaksięgowanie wszystkich znajdujących się w nim operacji – konieczne, by wszyscy użytkownicy sieci byli zgodni co do stanu

posiadania. Zgoda to inaczej konsensus. Konsensus jest sposobem na wybór konkretnego bloku spośród wszystkich proponowanych w sieci. Jak zatem działa konsensus?

Pierwszy algorytm konsensusu pracujący w publicznej sieci zaproponował – jak pewnie się domyślasz – Bitcoin. Wykorzystuje on bardzo prosty mechanizm. Spójrzcie na rewers dowodu osobistego. U dołu plastikowej karty znajduje się szereg znaków. Pośród dodatkowych cyfr i liter widnieje nasze imię i nazwisko, data urodzenia i numer dowodu. W tym momencie ważne są dla nas te dodatkowe cyfry. To tak zwana suma kontrolna, która zabezpiecza nasz dokument przed błędem lub oszustwem. Za jej pośrednictwem oprogramowanie wydawcy dowodu może szybko zweryfikować, i to bez dostępu do bazy obywateli, czy dowód jest prawdziwy. Dodatkowe cyfry to wynik obróbki danych zapisanych w dowodzie, końcowy wynik algorytmu, przez który je „przepuszczono". Na przykład jeśli oszust, podrabiając dowód, zmieni nasz wiek, oprogramowanie wykryje szwindel, bo suma kontrolna na dowodzie nie będzie się zgadzać z resztą informacji. Podobne mechanizmy zabezpieczające stosuje się w przypadku kart kredytowych, plików muzycznych czy zdjęć, głównie do wykrywania błędów, ale także do zabezpieczenia nas przed potencjalnym niebezpieczeństwem. Niezgodność sumy kontrolnej z wzorcową to sygnał, że z naszym plikiem coś jest nie tak, że – na przykład – do pliku muzycznego dopisał się jakiś wirus.

Suma kontrolna dobrze tłumaczy, jak działa konsensus Bitcoina. Zamiast naszego imienia, nazwiska, wieku, adresu czy listy piosenek mamy listę transakcji w bloku. Specjalne oprogramowanie wczytuje tę listę i przetwarza ją specjalnym algorytmem, który zwraca ciąg znaków. Wystarczy teraz, że zmienimy chociaż jedną literę zawartości bloku, a jego suma kontrolna zmieni się w ciąg znaków zupełnie niepodobny do

poprzedniego. To oczywiście tylko proste omówienie zasady – metoda na niej oparta i wykorzystywana w świecie kryptowalut oraz w oprogramowaniu komputerowym jest o wiele bardziej złożona, a nazywa się ją funkcją hashującą.

Funkcja hashująca – jak każda funkcja matematyczna – z tych samych danych wejściowych zawsze „wyprodukuje” identyczne dane wyjściowe, w tym wypadku ciąg znaków. Ale z tego ciągu znaków nie można odtworzyć danych, które go wygenerowały. Podobnie jak pijąc koktajl, nie wiemy, ile dokładnie truskawek i bananów zostało użytych do jego przygotowania, ani jakie jeszcze składniki i w jakiej ilości były w przepisie. Możemy za to bardzo dokładnie powiedzieć, czy ten koktajl nam smakuje, czy nie!

Po tym kulinarno-obywatelskim przygotowaniu wiemy już wszystko, co trzeba, by zrozumieć, jak działa konsensus Bitcoina. Bitcoin oficjalnie podaje, jaki koktajl mu smakuje. Górnicy, niczym barmani, do listy transakcji dodają losowe składniki i wykonują dość drogie miksowanie. Następnie sprawdzają, czy otrzymany przez nich koktajl jest dobry – to znaczy, czy będzie smakował Bitcoinowi.

Oczywiście to tylko przenośnia. Standard sieci kryptowalutowej dokładnie definiuje, jakie liczby wygenerowane w hashowaniu są dobre i zatwierdzają blok. Hashowanie przypomina trochę grę w totolotka. Nigdy nie wiemy, co wypadnie z nowego zestawu danych. Te „dobre” ciągi liczbowe zaczynają się od zer. Od określonej ich liczby – dziś jest to dziewiętnaście. Satoshi Nakamoto, twórca Bitcoina, wszystko policzył tak, żeby dobre ciągi pojawiały się co dziesięć minut. Pewnie zastanawiasz się, jak on to przewidział? Skąd wiedział, jak szybkie komputery będą za dziesięć lat? Przecież moc obliczeniowa wciąż się zwiększa! Sekret tkwi właśnie w tych dziewiętnastu zerach. Jeżeli bloki zostaną zatwierdzone za

szybko, protokół Bitcoina dokona samoregulacji i do zatwierdzania kolejnych bloków będzie wymagał dwudziestu zer na początku ciągu! I przeciwnie: przypuśćmy, że olbrzymia awaria zasilania pozbawia jakiś kraj prądu i odłącza pracujących w nim górników od sieci. Spada więc prędkość odgadywania rozwiązań bloku. Do zatwierdzenia kolejnego dochodzi dopiero po trzydziestu pięciu minutach. Protokół odczuwa to spowolnienie i zarządza zmniejszenie liczby wymaganych zer do takiej, która ustabilizuje czas zatwierdzania na poziomie zakładanych dziesięciu minut.

Czas na krótkie podsumowanie. W sieci kryptowalutowej co jakiś czas musimy zatwierdzić blok, który przypieczętowuje transakcje. Zatwierdzeniem bloku – wyborem bloku, który ma być uznany przez wszystkich za jedyny prawdziwy – zajmują się górnicy. Biorą oni listę transakcji i przetwarzają ją funkcją hashującą – w skrócie: hashują. Jeśli któryś z nich hashując jakiś blok, otrzyma ciąg cyfr zaczynający się od odpowiedniej liczby zer, to tenże blok zostaje rozgłoszony po sieci jako zatwierdzony. Jeśli hashowanie nie wygeneruje dobrego ciągu (z odpowiednią liczbą zer z przodu), wówczas górnicy do listy transakcji dodadzą losowy ciąg w specjalnie przeznaczonym do tego miejscu bloku i znów spróbują go hashować. Ten proces nazywa się kopaniem.

W wyniku kopania raz na mniej więcej dziesięć minut pojawia się szczęśliwy górnik, który prezentuje dobry blok. Cała sieć uznaje ogłoszoną przez niego kolejność transakcji i księguje wspólny stan posiadania.

Wróćmy teraz do naszego przykładu z Janem, Kasią i Lilią. Jeżeli szczęśliwy górnik otrzymał dobry ciąg, hashując blok z obiema transakcjami – między Janem a Kasią i Kasią a Lilią – to obie transakcje zostaną zaksięgowane przez wszystkie węzły w sieci. Jeśli jednak zatwierdzony blok zawiera tylko jedną transakcję – między Janem a Kasią –

to Lilia na pieniądze od Kasi będzie musiała poczekać kolejne dziesięć minut, aż inny górnik szczęściarz zatwierdzi blok z przelewem dla niej.

Koszty i organizacja wydobycia

Napisałem powyżej, że hashowanie jest drogie. Skąd biorą się jego koszty? Hashowanie zużywa moc obliczeniową komputera – to operacja matematyczna realizowana przez procesor. Oczywiście koszt pojedynczej takiej operacji jest znikomy, ale ilość prób, które musimy przeprowadzić, zanim otrzymamy dobry ciąg, jest gigantyczna. Na najmocniejszym pojedynczym komputerze znalezienie dobrego bloku trwałoby miesiącami. Wyobraź sobie, ile energii elektrycznej trzeba zużyć, żeby non stop przez całe miesiące zasilać procesor pracujący z maksymalną wydajnością. To są już spore koszty i spore zużycie energii. Osobny rozdział poświęcę bardzo ważnym aspektom ekologicznym kryptowalut.

Wróćmy jednak do kosztów. Rzecz jasna koszty kopania muszą być zwracane górnikom, dobrze by też było, gdyby na kopaniu dało się zarabiać. I tak jest w rzeczywistości. Każdy górnik, który „wydobędzie” rozwiązanie bloku i pierwszy rozgłosi je w sieci, otrzymuje nagrodę. Obecnie jest to 6,5 bitcoina, co przy jego bieżącym kursie (1 BTC ≈ 100 000 PLN) oznacza, że za rozwiązanie bloku otrzymamy około 650 tysięcy złotych. Trudno oszacować koszt „wykopania” dobrego bloku. Prawdopodobnie na sam potrzebny do tego prąd przeznaczymy jakieś 70 tysięcy złotych, do tego trzeba mieć odpowiednią infrastrukturę sprzętową, która będzie kopać wydajniej niż zwykły komputer. Kopanie to wieloletnie i kosztowne zobowiązanie, choć może okazać się zyskowne.

Ponieważ szanse samodzielnego rozwiązania bloku są znikome, górnicy zawiązują spółdzielnie. Do takiej spółdzielni można dołączyć nawet ze zwykłym laptopem. Nagroda za rozwiązanie bloku będzie wówczas proporcjonalna do mocy obliczeniowej, którą udostępniliśmy spółdzielni. Spółdzielnie, które dysponują dużą mocą obliczeniową, otrzymują nagrodę nawet co kilkanaście dni, co pozwala im racjonalnie zarządzać ich własną ekonomią. Górnicy często korzystają z wyspecjalizowanych procesorów, które potrafią wykonywać tylko jedno zadanie – hashować blok. Robią to taniej i szybciej niż procesory uniwersalne. To również ma ciekawe konsekwencje, do których jeszcze wrócimy.

Łańcuch bloków – raz jeszcze

Skoro już wiesz, skąd biorą się zaksięgowane bloki, to łatwo zrozumiesz, czym jest łańcuch bloków. Otóż każdy nowy, dobry, zaksięgowany blok zawiera w sobie nie tylko transakcje, ale także – o czym z oczywistych powodów jeszcze nie wspominałem – szczęśliwy ciąg cyfr reprezentujący poprzedni zatwierdzony blok. Tak właśnie tworzy się ich łańcuch. Łańcuch bloków, czyli blockchain.

Każdy górnik dobrze wie, który łańcuch dostępny w sieci jest najświeższy i zawiera ostatnie zatwierdzone operacje. Pewnie ty też już się domyślasz, który z możliwych łańcuchów jest najbardziej aktualny. Tak! Ten najdłuższy jest najnowszy. Gdyby w wyniku jakiegoś szczęśliwego zbiegu okoliczności nie jeden, a wielu górników zgadło rozwiązanie bloku, to i tak z czasem tylko jeden z nich stworzy łańcuch dłuższy niż inne, i to ten łańcuch zacznie być uważany za źródło prawdy w sieci kryptowalutowej.

Bitcoin – elektroniczne złoto

Metoda szukania konsensusu w sieci stosowana przez najstarszą i największą kryptowalutę, bitcoin, jest bardzo skuteczna. Ba, w praktyce sprawdza się o wiele lepiej, niż może to wynikać z teorii. Jest jednak krytykowana. Słusznymi argumentami przeciwko niej są jej powolność (mając do dyspozycji zawrotne prędkości przesyłu danych i szybkie komputery, godzimy się na księgowanie co dziesięć minut) i energochłonność (w dobie troski o środowisko zużycie prądu na kopanie kryptowalut nie jest zbyt dobrze postrzegane).

To tylko dwa główne zastrzeżenia. Pozostałe dotyczą rozmaitych aspektów technicznych, od których zależą nowe możliwości i zastosowania kryptowaluty. Zresztą to nie co innego, a właśnie te zastrzeżenia stały się wyzwaniem dla programistów, zaowocowały rozkwitem technologii blockchain i sprawiły, że obecnie istnieją dziesiątki tysięcy kryptowalut. Wiele z nich straciło stricte finansowy charakter i zaoferowało niespodziewane możliwości.

Lecz mimo upływu czasu i bujnego rozwoju DeFi, bitcoin wciąż pozostaje największą kryptowalutą – stanowi prawie połowę wartości całego rynku kryptowalut.

Inne niż bitcoin kryptowaluty nazywamy walutami alternatywnymi, w skrócie altcoinami. Największą z nich jest ethereum, której kapitalizacja wynosi mniej więcej połowę kapitalizacji bitcoina.

Pewnie zastanawiasz się teraz, dlaczego bitcoin po dziesięciu latach, przy napędzającej go starej technologii i tylu nowocześniejszych kryptowalutach, jest nadal tak wiele wart.

Po pierwsze, bitcoin odznacza się bardzo dużą decentralizacją. Jest systemem o wiele bardziej rozproszonym niż jakakolwiek inna

kryptowaluta i dzięki temu bardziej odpornym na ataki czy różne wypadki losowe.

Po drugie, krytykowane „przepalanie prądu” oznacza zużycie realnych zasobów i paradoksalnie może być traktowane jako zaleta. Dokładnie w tym entuzjaści bitcoina dopatrują się wewnętrznej wartości kryptowaluty. Utrzymanie sieci bitcoina stało się tak drogie, że ta kryptowaluta z systemu pieniądza elektronicznego przemieniła się w elektroniczne złoto. I w analogii do złota, bitcoinem nie zapłacimy za kawę, gdyż byłoby to zbyt drogie i zbyt wolne. Natomiast być może chcielibyśmy ulokować w tej kryptowalucie – podobnie jak w złocie – część naszych oszczędności.

Jan nie zapłacił Kasi w bitcoinach

Uff… Co to był za rozdział! Pełen nowych pojęć, metod i… nie ukrywajmy: dziwactw. Wyszliśmy od hipotetycznej sytuacji – konieczności zrobienia szybkiego przelewu. Sytuacja znana nam bardzo dobrze z życia codziennego. Umiemy szybko przelewać, mamy przelewy ekspresowe, BLIK-a, apki typu Revolut i tak dalej. My jednak chcieliśmy przekonać się, jak taki szybki przelew działa w świecie kryptowalut – świecie bez pośredników, strażników i gwarantów, czyli banków. Dowiedzieliśmy się, czym jest portfel, adres, klucz publiczny i prywatny oraz kryptografia asymetryczna. Poznaliśmy nowe znaczenie słowa „transakcja”. Znowu pojawił się tajemniczy (mam nadzieję, że coraz mniej!) blockchain, tym razem w nieco bardziej szczegółowej odsłonie – pisałem o zatwierdzaniu bloków wypełnionych transakcjami, sumach kontrolnych, funkcji hashującej i… górnikach, którzy przepalają mnóstwo prądu, paradoksalnie nadając tym samym bitcoinowi wartość fizyczną. Na koniec stwierdziliśmy,

że bitcoin jest niczym złoto: bardzo wartościowy, ale trochę niewygodny i ciut przestarzały. I chyba sam już podejrzewasz, że Jan raczej nie zapłacił Kasi za kawę w bitcoinach. Pewnie skorzystał z innej, szybszej kryptowaluty…

4

Jeszcze o bitcoinie

Nie bez powodu podstawy „mechaniki” kryptowalutowej omówiłem na przykładzie bitcoina. Nie tylko dlatego, że to pierwsza kryptowaluta w historii! Jej blockchain jest modelowy, zatwierdzanie bloków (kopanie) też, a jej decentralizacja idealnie realizuje marzenie o niezależności od nadrzędnych instytucji – czyli to, o co de facto chodzi w kryptowalutach. Jeśli zrozumiałeś podstawy działania bitcoina, dalej już będzie z górki.

Wiesz już, że bitcoin ma wady (do jednej z nich, czyli przepalania prądu, wrócimy za chwilę), ale też wiele zalet (choćby wartość, stabilność i olbrzymi udział w rynku). Inne projekty kryptowalutowe (altcoiny) to próby ulepszenia tego, w czym bitcoin nie domaga (jak na przykład szybkość transakcji).

Ale i sam bitcoin nie powiedział jeszcze ostatniego słowa.

Pomost

Żeby bitcoin działał, potrzeba prądu. Dużo prądu. W dobie powszechnej energooszczędności i dbałości o ekologię dla wielu to nie do

zaakceptowania. To nadzwyczajne przywiązanie tworu wirtualnego do zasobów świata rzeczywistego może jednak stać się pomostem do uwiarygodnienia innych, mniej prądożernych systemów wirtualnych. Spalamy prąd, by nadać wymierną wartość wirtualnej monecie i udowodnić nasze zaangażowanie w jej utrzymywanie. Teraz tę monetę możemy wykorzystać w charakterze gwaranta wartości innej monety w równoległym systemie kryptowalutowym, nowocześniejszym, szybszym, bardziej ekologicznym. To niezwykle ciekawe, jak domyka się ten cykl: od nowej waluty (bitcoin), przez środek utrzymania wartości (prąd potrzebny do działania sytemu), po pomost zaufania łączący tę wartość z nową, lepszą kryptowalutą.

Spalenie stosu dolarów

Chcę w tym miejscu podkreślić, że owo przekleństwo bitcoina, czyli spalanie prądu, jest tak naprawdę przełomowym powiązaniem świata rzeczywistego ze światem wirtualnym. Dlaczego?

Wyobraźmy sobie, że tworzymy jakąś nową walutę i jako dowód naszego zaangażowania będziemy spalać stosik dolarów. Sytuacja na pierwszy rzut oka analogiczna do przepalania prądu w przypadku bitcoina – i tam, i tu koniec końców spalamy pieniądze. Tylko jak powiązać przepalanie dolarów z wartością naszej nowej monety? Choćbyśmy płonące banknoty filmowali na dowód nieodwracalnego zaangażowania w nadawanie wartości naszej dziwnej walucie, w dobie deepfake’u, wyrafinowanego montażu wideo i komputerowo generowanej grafiki taki film nie stanie się nigdy żadnym dowodem konwersji dobra rzeczywistego na wirtualne.

W przypadku bitcoina mamy do czynienia z czymś diametralnie innym. Prąd jest tu potrzebny, by napędzać całą tę zaawansowaną matematyczno-kryptograficzną maszynerię, służącą do zatwierdzania bloków z transakcjami i dołączania ich do łańcucha; wszystko po to, by zapewnić transakcjom bezpieczeństwo i uwolnić się od banku – centralnego strażnika i gwaranta obdarzanego społecznym zaufaniem – który jednak z naszymi pieniędzmi i przelewami może w teorii zrobić, co tylko uzna za stosowne. Jasne, wiąże go prawodawstwo uchwalane przez państwo, ale bywa, że owo prawodawstwo staje się niezgodne z wolą społeczeństwa – choćby w demokracjach staczających się ku ustrojom autorytarnym i dyktatorskim.

Bezpieczeństwo

Geniusz Satoshiego Nakamoto ujawnił się w wielu aspektach bitcoina, ale jednym z najważniejszych jest zapewnienie bezpieczeństwa wymyślonej przez niego kryptowaluty, i to w warunkach, w których o to bezpieczeństwo jest najtrudniej.

Jako młody programista zajmowałem się bazą danych w dużym komunikatorze internetowym. Miał on kilkaset milionów użytkowników. Nie istnieje baza, która zdołałaby obsłużyć taki ruch na pojedynczym komputerze. Bazy będące w stanie sprostać takiemu zadaniu działają – podobnie jak system bitcoina – na wielu węzłach sieci, na wielu komputerach.

Możesz mi wierzyć albo nie, ale mimo że nasza baza danych działała na bezpiecznych komputerach połączonych szybkimi i stabilnymi łączami, to pracowaliśmy w kilkudziesięcioosobowym zespole, który miał cały czas ręce pełne roboty polegającej na usuwaniu problemów, które pojawiały się

w sieci. A nie musieliśmy się przecież borykać z przebiegłymi oszustami czyhającymi na cudze oszczędności! Walka z nieuchronnymi awariami destabilizowała nawet najwydajniejsze algorytmy do ustalenia prawdy w naszej sieci, a w rozległych systemach takie awarie zdarzają się co kilkadziesiąt sekund.

Dlatego też nikomu z nas nawet przez myśl nie przeszło, że system rozproszonej bazy danych może dobrze działać w publicznej sieci między nieznającymi siebie węzłami – w warunkach sieciowej niestabilności i przy anonimowych użytkownikach.

Satoshi Nakamoto uruchomił system obsługujący jeden z najważniejszych aspektów naszego życia – finansów – w sieci publicznej. System z definicji narażony na oszustwa i ataki trafił i zaczął działać tam, gdzie o oszustwa i ataki najłatwiej.

Wynalazek Nakamoto – blockchain – oraz pierwsza kryptowaluta – bitcoin – pokazały, że coś tak niewiarygodnego, jak wrażliwy system w publicznej sieci, jest możliwe. Wywołało to rewolucję w naszych umysłach. Zdjęło ograniczenia myślenia.

Bitcoin ma już dwanaście lat. Około siedmiu lat temu rozpoczęły się prace nad *Proof of Stake* (dosłownie: Dowód Udziału) – algorytmami górniczymi służącymi do osiągania konsensusu (ustalania prawdy) w sieciach kryptowalutowych, nieco innymi niż opisane w poprzednim rozdziale prądożerne kopanie bitcoinów z wykorzystaniem funkcji hashującej. Ale dopiero zupełnie niedawno, dzięki najnowszym zdobyczom kryptografii, zaczęły one działać bez zarzutu. Teraz zabezpieczają gigantyczne operacje finansowe tanio, bezpiecznie i… ekologicznie!

To dzięki Satoshiemu Nakamoto dokonaliśmy gigantycznego skoku technologicznego w świecie wirtualnym i przeszliśmy do kolejnego etapu ewolucji finansów, pieniędzy i walut.

Fundamentalne prawo człowieka

Teraz, kiedy znasz już podstawy technologii blockchain, na pewno będziesz w stanie docenić jej zalety.

Zawsze powtarzam, że nieskrępowany dostęp do własnych finansów to fundamentalne prawo człowieka, zapewniające mu niezależność i samostanowienie.

Pomyśl tylko, jaką rewolucję blockchain wywoła w krajach, w których całe grupy społeczne (na przykład kobiety czy mniejszości etniczne) są wykluczone z systemu finansowego. Już teraz dzięki zdecentralizowanym kryptowalutom osoby potrzebujące w opresyjnych państwach mogą otrzymać pomoc pieniężną, a uchodźcy wydostać się z nich z oszczędnościami życia.

Z punktu widzenia przeciętnego Europejczyka takie przykłady to czysta abstrakcja. Zatem po co nam blockchain?

Pewnie właściciele kont w bankach na Cyprze, państwie, które zbankrutowało w 2013 roku, doceniliby wyłączną osobistą kontrolę nad własnymi środkami.

Cypr znacjonalizował wszystkie oszczędności powyżej objętych europejską gwarancją bankową stu tysięcy euro. Coś podobnego w zdecentralizowanym systemie kryptowalutowym jest absolutnie niemożliwe, ponieważ środki posiadamy wyłącznie my – i to my sprawujemy nad nimi pełną kontrolę. Nie ma tu strażnika, który pewnego dnia może postanowić, że twoje oszczędności zostaną przekazane na ratowanie kraju z finansowej zapaści, po czym usunie je z należących do ciebie kont bankowych.

Gdyby w finansach rządziły kryptowaluty, spokojniejszy sen mieliby mieszkańcy Turcji. W 2021 roku systemowo przymuszano ich do zmiany

stanu kont z obcą walutą i wykupu krajowej, kiedy turecka lira zaczęła ostro pikować w dół. W zdecentralizowanym pseudoanonimowym systemie wprowadzenie takiego przymusu okazałoby się zdecydowanie trudniejsze niż kliknięcie myszą przez szefa banku centralnego.

Spójrzmy na Rosję i jej barbarzyńską agresję na Ukrainę – graniczący z nami nowoczesny, rozwijający się kraj o europejskich aspiracjach. Świat zachodni nakłada na Rosję gigantyczne sankcje, kurs rubla spada o połowę w jeden dzień, a indeks moskiewskiej giełdy o 38% – to rekord w historii światowego handlu giełdowego. Chcąc ustabilizować kurs rubla, rosyjskie ministerstwo finansów utrudnia jego wymianę, jak może. Konwersję rubla na obce waluty obciąża kilkudziesięcioprocentową dodatkową marżą, a eksporterów obliguje do natychmiastowej wymiany ich dolarów, funtów i euro na kopiejki. Takie centralne regulacje rynku finansowego nie miałyby żadnego wpływu na zdecentralizowany system kryptowalut.

I jeszcze Kanada, rok 2022. Trwają protesty obywatelskie przeciw obostrzeniom z powodu covidu. W wielu miastach są organizowane miasteczka protestacyjne. Przez Kanadę przejeżdża słynny na cały świat wielokilometrowy konwój.

I już w tym miejscu zastrzegam, że nie chcę oceniać ani słuszności tych protestów, ani słuszności walki z nimi. Nie chcę wartościować działań żadnej ze stron sporu. Pragnę tylko pokazać, do czego może posunąć się nowoczesne, demokratyczne, zachodnie państwo, dysponujące pełnią władzy nad finansami obywateli. Otóż premier Justin Trudeau zaproponował projekt ustawy zamrażającej – bez procesu sądowego – środki finansowe na kontach zidentyfikowanych protestujących. Taki precedens szokuje – łatwo sobie wyobrazić, jak ogromne otwiera się tu pole do nadużyć i jak duża może być pokusa, by iść na skróty. A przecież można było wszystko załatwić w ramach obowiązującego już prawa.

We wszystkich powyższych przykładach zdecentralizowany system finansowy chroniłby obywateli przed zakusami rządzących i instytucji. Unikalny adres portfela, niepowiązany z tożsamością obywatela, a jednocześnie do niego przypisany, to prosta recepta na swobodny dostęp do własnych finansów, który, jak już pisałem, jest według mnie jednym z podstawowych praw człowieka.

Dlaczego? Choćby dlatego, że na protest – manifestację obywatelskiego sprzeciwu – trzeba dojechać (tankowanie, bilety), a potem przez jakiś czas utrzymać się poza domem. Jeśli nie dysponujemy gotówką, zamrożenie środków na koncie skutecznie utrudni wyrażenie naszego niezadowolenia z prowadzonej polityki. A w dobie miejskich kamer rozpoznających tożsamość wprost z obrazu podjęcie takich działań przez państwo staje się dziecinnie proste i możliwe od ręki.

Inny przykład, tym razem z branży hazardowej. Kilka lat temu zostało w USA zmienione prawo regulujące grę w pokera, który w wersji online rozrósł się do takiej skali, że praktycznie stał się gałęzią przemysłu. Mnóstwo osób – profesjonalnych graczy – zaangażowało w tę grę większość swoich środków, czyniąc ją głównym źródłem swojego utrzymania. Z dnia na dzień dostęp do ich kont został zablokowany. Zgromadzone na nich środki przepadły. Tu strażnikiem i gwarantem były prywatne firmy pokerowe online. Gdyby gracze korzystali ze zdecentralizowanej waluty, zachowaliby zgromadzone środki. Przecież prawo nie powinno działać wstecz.

A niesienie pomocy? Rozmaite trudności techniczne mogą je udaremnić nawet w XXI wieku. Wiele organizacji charytatywnych ze Stanów Zjednoczonych nie może przetransferować oficjalnymi kanałami środków do krajów trzeciego świata tak, by trafiły do potrzebujących rodzin. Na przeszkodzie stoją zwykle polityka i sankcje. Tymczasem niektóre

organizacje charytatywne przyznały, że transfer kryptowalut pozwolił im ominąć wspomniane przeszkody, dzięki czemu pomoc finansowa sprawnie dotarła tam, gdzie była potrzebna.

Raj dla przestępców?

Z jednej strony zdecentralizowane systemy stają w obronie praw jednostki, ale z drugiej osłabiają mechanizmy kontroli państwowej. Czy zatem blockchain może stać się rajem dla przestępców?

Nie. Jak pokazują wyniki badań, tylko jeden procent kryptowalutowych transakcji nosił znamiona nielegalności – to aż cztery razy mniej niż w tradycyjnym systemie finansowym. Pamiętaj, że blockchain jest systemem pseudoanonimowym, na którego „obrzeżach" działają giełdy pozwalające wymienić kryptowalutę na tradycyjne waluty. Wszystkie takie giełdy działają na mocy licencji państwowych i tu kończy się anonimowość użytkowników. Obecny rozmiar rynku kryptowalut jest również zbyt mały, by mógł sobie pozwolić na omijanie ogólnopaństwowych sankcji – styk świata wirtualnego z rzeczywistym można łatwo kontrolować, niczym krótki odcinek granicy.

Kryptowaluty tworzą swoją równoległą ekonomię i równoległy świat. Ich wielość i różnorodność sprawiają, że znajdziemy wśród nich zarówno projekty nawiązujące do libertariańskiego *Manifestu Cypherpunków* i zapewniające prawdziwą anonimowość, jak i takie, które są częścią absolutnie scentralizowanego systemu zbierania punktów za tankowanie na stacji należącej do dużej sieci.

Portfel – rady praktyczne

1. Dwaj uznani producenci portfeli sprzętowych to Ledger oraz Trezor. Oferują urządzenia chroniące klucz prywatny. W odróżnieniu od choćby przenośnego dysku lub pendrive'a, kiedy takie portfele sprzętowe dostaną się w niepowołane ręce, nie pozwolą na odczyt klucza prywatnego (nawet za pomocą mikroskopu czy narzędzi do łamania haseł).

2. Istnieją portfele fizyczne mające postać kart kodujących lub metalowych blankietów, na których graweruje się lub wybija klucz prywatny. Jest on kodowany 12 lub 24 słowami. Karty rozdzielające klucz pozwalają zdeponować jego fragmenty w kilku miejscach – na przykład u adwokata, u notariusza, u babci, w termosie zakopanym w ogródku i tak dalej. W zależności od metody generowania takiego zabezpieczenia możemy określić, ile części potrzeba do odtworzenia pełnego klucza.

3. Portfel sprzętowy łączymy z systemem przez port USB lub zbliżeniowo za pomocą technologii NFC. W portfelu wybieramy walutę, po czym generuje się dla nas adres. Dla każdej nowej transakcji możemy wygenerować oddzielny adres kontrolowany przez ten sam portfel. Portfela używamy do zakończenia każdej transakcji poprzez podpisanie jej kluczem prywatnym z portfela.

4. Metoda dwuetapowej weryfikacji (2-FA) jest podstawowym sposobem zabezpieczenia każdego konta. Drugi etap zwykle polega na wprowadzeniu kodu z innego urządzenia należącego do właściciela portfela. Na przykład logując się na komputerze, w drugim kroku wprowadzamy kod przesłany na nasz telefon. Uwaga – unikamy metod z przesyłaniem kodu przez SMS! Przejęcie numeru GSM jest niestety trywialne. Używajmy dedykowanej aplikacji autoryzującej – choćby od Google'a. Jeśli nasze konta nie są zabezpieczone dwuetapową weryfikacją, w żadnym wypadku nie możemy uznać ich za bezpieczne – dotyczy to nie tylko kryptowalut.

5. Wyższy stopień bezpieczeństwa oferują dedykowane urządzenia do przesłania kodu dwuetapowej weryfikacji, na przykład Yubikey. Są

mniejsze niż pendrive’y. Obsługujemy je zbliżeniowo lub przez port USB i naciśnięcie klawisza.

5

Giełdy

– Słuchaj, taka sprawa… Jak się rozliczacie po treningu? Nie znam zbyt dobrze tych ludzi i nie chcę im podawać swoich danych… A trochę mi głupio zwlekać z płatnością za salę…

– My używamy jednego z tokenów. Masz swój portfel?

– Tokeny? Portfel? No… mam portfel, ale nie myślałem, że będziemy się rozliczać gotówką.

– Chodzi o portfel kryptowalutowy! Nie korzystasz?

– A, kryptowaluty… Nie, nie korzystam, słyszałem o nich co prawda, bo trudno nie słyszeć dziś o kryptowalutach, ale to dla mnie czarna magia. Warto w to wejść?

– Warto, warto. Jeśli chcesz zacząć używać kryptowalut, to szybko ci powiem, co i jak. Na początku będzie trochę formalności, bo musisz zarejestrować się na jakiejś giełdzie. Najlepiej wybrać giełdę w stabilnym, godnym zaufania, praworządnym kraju, na przykład w Stanach, Anglii, Niemczech, Szwajcarii… Dość duże giełdy znajdziesz w Korei Południowej i Japonii. Giełda poprosi o twoje dane osobowe, a do odblokowania większych płatności będziesz im musiał przesłać dokument tożsamości. Zwykle wystarcza skan dowodu osobistego zrobiony kamerą smartfona lub laptopa. No i ważne jest, żeby firma zarządzająca wybraną przez ciebie giełdą była publiczna, czyli notowana na giełdzie – to znaczy zwykłej giełdzie papierów wartościowych – i zweryfikowana przez państwowe urzędy.

– Czyli muszę założyć konto… Jak na przykład w serwisie społecznościowym?

– No, mniej więcej. Tyle że na to konto przelejesz swoje pieniądze. W jednej z zakładek swojego giełdowego profilu znajdziesz metody zasilenia konta. I za taki przelew zwykle nie pobierają prowizji.

– Czyli przelewam środki ze swojego konta bankowego na swoje konto giełdowe. Zupełnie jak u brokera giełdowego!

– O właśnie, dokładnie jak u brokera. I tak samo jak na zwykłej giełdzie papierów wartościowych wymieniasz pieniądze na akcje, tu będziesz mógł wymienić tradycyjną walutę na tokeny kryptowalutowe. Jest jednak zasadnicza różnica. Twoje tokeny zostaną przesłane na twój giełdowy adres. Nie masz do niego klucza, który zabezpiecza wszystkie transakcje. Dlatego dobrze przesłać je od razu do portfela, który sam założysz w przeglądarce lub smartfonie. I wtedy staniesz się już całkowicie niezależny.

– A co zabezpiecza mój portfel?

– Kryptografia, czyli kawał zaawansowanej matematyki. Dzięki niej włamanie się do portfela i dokonanie nieautoryzowanego przelewu jest praktycznie niemożliwe. Poza tym twój prywatny portfel może być używany do wielu zadań, nie tylko do przechowywania tokenów. Giełda to koniec końców zwykła firma – jedną ze świadczonych przez nią usług jest pomost między światem zwykłych walut i kryptowalut.

Skąd się biorą i skąd brać kryptowaluty?

Giełdy. Firmy działające na styku pieniądza zwykłego i elektronicznego. Najprostszy sposób zakupu kryptowalut. To tam wymieniamy złote, euro, dolary i wszelkie inne klasyczne waluty na tokeny, czyli monety kryptowalut: bitcoina, ethereum i innych. Ostatnio wiele aplikacji finansowych – takich jak PayPal i Revolut – również pozwala kupić tokeny najpopularniejszych kryptowalut. Na obecnym etapie rozwoju nie mogą jednak zastąpić giełdy – można w nich tylko kupować i sprzedawać tokeny kryptowalut za zwykłą walutę, w dodatku od każdej takiej transakcji pobierana jest prowizja. Zakupionej w Revolucie czy PayPalu kryptowaluty

nie będziesz mógł wytransferować do swojego portfela ani swobodnie z niej korzystać na co dzień, jak choćby w przykładzie rozpoczynającym niniejszy rozdział. Znacznie lepiej rozpocząć przygodę z kryptowalutami, dysponując wszystkimi potrzebnymi narzędziami i mając nad nimi pełną kontrolę. Co nie jest znowu aż takie trudne.

Skąd właściwie biorą się kryptowaluty na giełdach? Jeden mechanizm zdążyłeś już poznać. Górnicy, którzy odpowiadają za spójność sieci, czyli za zatwierdzanie bloków w blockchainie (by wszystkie wszędzie były takie same), otrzymują nagrody w postaci tokenów. Chcąc zapłacić za prąd tradycyjną walutą, muszą te tokeny na nią wymienić, czyli sprzedać. I tak właśnie rozpoczyna się wymiana. Cenę walut reguluje prawo popytu i podaży.

Nowe generacje blockchainów, które nie wymagają takiego prądożernego kopania jak w przypadku bitcoina, również wynagradzają zatwierdzających bloki uczestników sieci. Ten mechanizm wypłat za utrzymywanie sieci danej kryptowaluty to wspólny i podstawowy sposób zasilania sieci w nowe tokeny.

Czy pojawianie się nowych monet nie napędza aby inflacji? Czy nie jest to coś podobnego w skutkach do dodrukowywania pieniędzy? I tak, i nie. Już wyjaśniam.

Każda kryptowaluta w swoim protokole dokładnie precyzuje, ile powstanie tokenów i kiedy. Na przykład liczba bitcoinów jest stała: wynosi 21 milionów. Nagrody dla górników zmniejszają się o połowę co każde 210 tysięcy bloków, czyli co cztery lata. Bitcoin zatem przejawia cechy deflacyjne – wzrasta jego siła nabywcza (nowego pieniądza jest na rynku coraz mniej, pensje górników w sposób zaplanowany maleją).

Deflacja nie jest tu jednak regułą. Wręcz przeciwnie. Wiele systemów kryptowalutowych szczodrze wypłaca monety. Zwykle dzieje się tak, gdy

waluta jest młoda: wówczas inflacja w systemie jest wysoka – wysokie wypłaty przyciągają nowych uczestników i zachęcają ich do zatwierdzania bloków i stabilizowania sieci. Następnie – po miesiącach lub latach – inflacja zmniejsza się do wartości dobrze znanych z teorii ekonomii i wynosi od jednego do pięciu procent.

Teraz już chyba w pełni rozumiesz jedną z przyczyn stabilnej wartości najstarszej kryptowaluty – bitcoina. Jest jak elektroniczne złoto. Stabilny. Pożądany. Zawsze w cenie.

Aby zwiększyć zainteresowanie nową kryptowalutą, jej twórcy czasem organizują airdrop, czyli zrzut z powietrza – chętnym lub losowo wybranym osobom rozdają monety i zachęcają do ich wydania, na przykład w biorącym udział w akcji serwisie streamingowym z muzyką lub filmami. To znana strategia marketingowa i kojarzysz ją na pewno z życia codziennego – różne firmy często organizują w sieci konkursy, w których nagrodami są ich produkty, zwykle te debiutujące na rynku: nowe modele słuchawek, smartfonów, premierowe książki czy abonamenty rozmaitych serwisów.

Airdropy są bezpieczne – pod warunkiem zachowania elementarnej ostrożności. Oszuści mogą wykorzystać chęć zdobycia monet za darmo do wyłudzenia kluczy lub do zainfekowania komputera ofiary. Ale to też nic nowego – w „zwykłym” internecie również pojawiają się podejrzane konkursy lub bardzo okazyjne wyprzedaże. Atrakcyjne nagrody lub luksusowe towary za bezcen przyciągają amatorów szybkiego wzbogacenia się. Zawsze trzeba mieć oczy szeroko otwarte. W każdym razie airdropy to coś zupełnie normalnego – uznana praktyka marketingowa, której nie musimy się obawiać, a możemy na niej skorzystać.

Innym sposobem wprowadzenia nowych tokenów do obiegu jest powołanie ich do życia. Można to zrobić tylko raz – kiedy powstaje nowy

blockchain. Bardzo często w przypadku nowych kryptowalut w ich pierwszym bloku – tak zwanym bloku Genesis – deklarowana jest pierwotna własność przedsięwzięcia. Przydziałem, który ją określa, jest wynagrodzenie inwestorów finansujących budowę nowej sieci. Wynagrodzenie to wypłacane jest jej tokenami.

Myślę, że łatwiej będzie zrozumieć to na prostym przykładzie.

Kryptowalutowa wypożyczalnia Karola

Wyobraźmy sobie przedsiębiorczego Karola. Karol chce założyć wypożyczalnię sprzętu sportowego w miasteczku studenckim. Chce przyjmować płatności w nowej, stworzonej przez siebie kryptowalucie. Obliczył, że w cały interes musi zainwestować milion złotych. Ta suma to nie tylko koszt samego sprzętu do wypożyczania. Z tej kwoty musi sfinansować zakup komputerów, na których stworzy swoją nową kryptowalutę, ale także wynagrodzenie ekipy informatyków, marketingowców i prawników.

Karol ogłosił zbiórkę na swój start-up – można zostać udziałowcem w biznesie Karola, inwestując w niego bitcoiny. Załóżmy teraz, że bitcoinowa zrzutka zakończyła się sukcesem.

Mija kilka miesięcy. W tym czasie Karol tworzy nową sieć kryptowalutową – prace nad nią finansuje ze sprzedaży zebranych bitcoinów. Ta sieć na razie nie jest znana, więc jej kryptowaluta nie jest wiele warta. Mimo to wszyscy inwestorzy, którzy swoimi bitcoinami zasponsorowali jej powstanie, otrzymują wygenerowane w niej tokeny – zostaną im one przydzielone w bloku Genesis proporcjonalnie do wniesionych w bitcoinach udziałów.

Czy nie przypomina to przypadkiem zwykłej spółki akcyjnej? Owszem, ale udziały w spółce kryptowalutowej – wyrażone w otrzymanych tokenach – zasadniczo się różnią od akcji spółki akcyjnej. Chodzi o użyteczność. Tradycyjne akcje odzwierciedlają, jaką część firmy posiadamy. Tymczasem tokeny są nie tylko płynnym wyznacznikiem naszego stanu posiadania, ale także użytecznym instrumentem – w naszym przykładzie za pomocą tokenów będzie można wynająć rowery i inny oferowany przez wypożyczalnię sprzęt.

Szeroko zakrojona akcja promocyjna wypożyczalni Karola, połączona z airdropem nowej waluty, przynosi efekty. Jest całkiem sporo chętnych do skorzystania z nowego punku usługowego w kampusie – szczególnie że sprzęt jest pierwsza klasa, a bezgotówkowe płatności kryptowalutowe to ostatni krzyk mody. Studenci odszukują nowe tokeny na giełdzie, wymieniają na nie posiadaną kryptowalutę: bitcoiny, ethereum i tym podobne (kurs jest bardzo korzystny!) i zasilają nimi swój portfel kryptowalutowy. W ten sposób tworzą popyt na kryptowalutę Karola i jej wartość zaczyna wzrastać.

W tym przykładzie mamy happy end, a nawet dwa. Pierwszy to udana zbiórka bitcoinów na powstanie nowej kryptowaluty. Drugi – biznes Karola ruszył z kopyta i nadał tej nowej kryptowalucie wartość, bo dzięki wypożyczalni pojawił się na nią popyt. Tymczasem w rzeczywistości tylko nieliczne z takich przedsięwzięć się udają. Stworzenie nowej kryptowaluty to proces nie tylko czasochłonny i skomplikowany, ale i ryzykowny z czysto biznesowego punktu widzenia.

Stary świat w nowym świecie

Giełdy i mechanizmy tworzenia płynności w świecie blockchainów… Chyba sam już dostrzegasz, że są one zaskakująco podobne do tradycyjnych sposobów wymiany dóbr. Sami jesteśmy trochę temu winni – na nowy grunt staramy się przenosić stare wzorce. Bo dobrze je znamy.

Opisywałem tu działanie giełdy, czyli prywatnego przedsiębiorstwa umożliwiającego wymianę różnych kryptowalut oraz ich zakup i sprzedaż za klasyczne waluty. Taka giełda to twór scentralizowany, a jak dobrze wiesz, centralizacja stoi w sprzeczności z naczelną ideą kryptowalut, czyli decentralizacją. Zderzają się tu zresztą nie tylko centralizacja i decentralizacja, ale także anonimowość z jawnością: zapewne pamiętasz z przykładu otwierającego ten rozdział, że aby skorzystać z usług giełdy, trzeba się na niej zarejestrować, wysyłając swoje dane osobowe i czasem skan dokumentu tożsamości. Giełda łączy więc naszą wirtualną tożsamość z tą prawdziwą. Jeśli przywołamy w tym miejscu fakt, że wszystkie operacje w blockchainie są publiczne, jasne się stanie, że twierdzenia, jakoby blockchain służył do malwersacji czy prania brudnych pieniędzy, są nieuprawnione. Blockchain to w rzeczywistości jedno z gorszych miejsc do przeprowadzania nielegalnych operacji finansowych i dlatego ich odsetek jest w przypadku kryptowalut kilkukrotnie mniejszy niż w świecie klasycznych finansów. Owszem, istnieją co prawda blockchainy w pełni anonimizujące operacje, ale ich płynność jest znikoma.

W tym miejscu wspomnę tylko, że istnieją też zdecentralizowane giełdy. Ich działanie to jednak bardzo złożony mechanizm, szczególnie dla osoby, która dopiero rozpoczyna swoją przygodę z kryptowalutami. Nie będę zatem szczegółowo ich opisywał. Pamiętaj jednak: zdecentralizowane giełdy to następny krok w rozwoju systemów kryptowalutowych.

Wspomniałem, że giełdy kryptowalutowe to tak jakby wytwór starego świata przeniesiony na nowy grunt. Drugim takim artefaktem – ściśle

związanym z giełdami – są tak zwani *market makers*. Polskie tłumaczenie tego terminu to „animatorzy rynku” i chyba trochę lepiej oddaje sens ich działalności.

Animatorzy rynku korzystając ze swoich rezerw, nadają płynność i powodują, że skraca się czas oczekiwania na zawarcie transakcji, w szczególności tych związanych z wymianą niezbyt popularnych kryptowalut. Mówiąc w uproszczeniu: czasami kupują to, czego nikt inny raczej by nie kupił, i w ten sposób „animują” rynek – troszkę i właściwie to tylko na chwilę fałszując jego obraz przez wywoływanie sztucznego zainteresowania nieznanymi tokenami i tym samym zwracając na nie uwagę.

Tutaj jednak mam bardzo dobrą wiadomość: w zdecentralizowanym świecie animatorzy rynku są… automatyczni. Ten przełomowy wynalazek przysłużył się wszystkim uczestnikom handlu na giełdach kryptowalutowych i zdemokratyzował nadawanie płynności rynkowi. Każdy z nas może wydelegować swoje oszczędności do automatycznego animatora rynku (jest nim specjalny algorytm) i być beneficjentem potencjalnych, wygenerowanych przez niego zysków. Cały proces jest transparentny i stanowi kolejny kamień milowy w rozwoju kryptowalut.

Giełdowe przekręty

Wspomniałem, że idea centralnej giełdy – firmy, która działa na styku pieniądza rzeczywistego i wirtualnego – kłóci się z decentralistyczną koncepcją kryptowalut. Jakie konkretnie są negatywne konsekwencje centralizacji? Na przykład takie, że użytkownicy giełdy nie przejmują się zbytnio bezpieczeństwem i zawierzają jej ochronę swoich funduszy.

Korzystają z wygenerowanego przez giełdę klucza prywatnego i nie kontrolują zainwestowanych środków portfelem sprzętowym. Giełdy są serwisami – strażnikami (widzisz, jak niebezpiecznie zbliżamy się do idei banków, którą tak bardzo chcieliśmy wyeliminować ze świata kryptowalut) chroniącymi gigantyczne ilości monet. To zaś czyni je celem ataków i nadużyć. I niestety takie ataki i nadużycia niejednokrotnie się już zdarzały.

Pierwszym głośnym przypadkiem – ze względu na rozmiar strat – było przejęcie giełdy Mt.Gox w 2014 roku. Klienci giełdy stracili 740 tysięcy bitcoinów, a sama giełda 100 tysięcy – sumarycznie była to wówczas równowartość 460 milionów dolarów. Dziś to ponad 17 MILIARDÓW! Część środków została odnaleziona przez syndyka w tak zwanych zimnych portfelach, które są odizolowane od sieci, przez co sieciowi przestępcy nie mają do nich dostępu. Był to drugi atak w historii giełdy Mt.Gox; pierwszy zdarzył się trzy lata wcześniej. W śledztwie wykryto sporo nieprawidłowości działania giełdy, na przykład to, że w firmie nie stosowano żadnych dobrych praktyk tworzenia oprogramowania.

Innym giełdom – takim jak KuCoin, Upbeat, Binance, Coinbene, Coincheck – zdarzało się tracić od kilkunastu do kilkuset milionów dolarów. Radziły sobie na różne sposoby: pokrywały straty z funduszu bezpieczeństwa lub inicjowały policyjne śledztwa, które w wyniku analizy transferów w końcu namierzały winowajców.

Przez ostatnią dekadę skradziono z giełd prawie trzy miliardy dolarów. Główną przyczyną jest przechowywanie zbyt dużych środków w podręcznych portfelach.

Na szczęście niedawno na rynku pojawiły się korporacyjne rozwiązania, które nie tylko opierają się na lepszym oprogramowaniu, ale także skutecznie zabezpieczają przepływ informacji w firmach i pozwalają na

pełną kontrolę zmian dokonywanych w wyniku transakcji. Co jakiś czas pojawiają się sensacyjne doniesienia o włamaniach na giełdy, jednak wbrew temu, co można sądzić, wartość strat zdecydowanie zmalała.

Podsumowując: prawo dotyczące giełd kryptowalutowych musi być jasne, klarowne i stymulujące rozwój tej branży – tylko tak doprowadzimy do tego, że przestaną być zakładane w szemranych jurysdykcjach. Dobre prawo usprawni kontrolę nad operacjami w blockchainie. Państwa, które poważnie i preferencyjnie potraktują giełdy kryptowalutowe, zyskają świetne źródło podatku!

Zresztą już teraz największe giełdy kryptowalutowe grają w tej samej lidze co ich tradycyjne odpowiedniki. Na przykład giełda Coinbase jest publicznie notowana i warta 48 miliardów dolarów. Dla porównania: London Stock Exchange (LSE), czyli londyńska giełda papierów wartościowych, jest warta 57 miliardów dolarów. Pisałem o stratach, ale zdarzają się też pozytywne, optymistyczne historie. W maju 2017 roku bułgarska policja aresztowała 23 członków grupy przestępczej, która wykorzystując wirusy, dokonywała kradzieży środków finansowych z prywatnych oraz państwowych kont i lokowała je w bitcoinach. W wyniku policyjnej operacji SHIPMENT/VIRUS przejęto ponad 200 tysięcy bitcoinów! Bułgaria stała się wówczas jednym z największych posiadaczy bitcoina na świecie. Niestety, nie podano szczegółów, co się stało z tymi monetami wartymi w dniu konfiskaty miliard dolarów, a dziś… ponad 4,5 miliarda! Zresztą już w grudniu tego samego roku, w którym przejęto brudne bitcoiny, ich wartość skoczyła do 3 miliardów dolarów – było to aż 18% długu narodowego Bułgarii! Kiedy zaś bitcoin osiągnął szczyt notowań 14 kwietnia 2021 roku, wartość przejętych środków przekroczyła 10 miliardów dolarów. Oficjalnie rząd Bułgarii spieniężył je partiami, żeby nie destabilizować rynku. Hm… Planowany budżet Bułgarii

w 2017 wynosił niemal 23 miliardy dolarów, a w 2022 – 33 miliardy. Możemy tylko zgadywać dlaczego…

Ale jak w ogóle przejęto te bitcoiny? Nie wiadomo. Wyobrażam sobie taką sytuację (to oczywiście skrajny przypadek): karteczka przylepiona do monitora… Na niej zapisane hasło do portfela… Jedno zdjęcie smartfonem… Pozostają nam tylko domysły.

Inną, zdecydowanie słynniejszą akcją rządową, choć z mniejszą wartością przejętych środków, było zamknięcie w 2014 roku nielegalnej giełdy Silk Road i konfiskata 44 tysięcy bitcoinów. W przeciwieństwie do przypadku bułgarskiego, tu mieliśmy jasność, co się stało z brudnymi monetami. Agencje USA dość transparentnie upłynniają przejmowane kryptowaluty.

Największe kontrowersje wokół tej sprawy skupiają się na operatorze giełdy Rossie Ulbrichcie. Postawiono mu zarzuty nielegalnego obrotu pieniędzmi i organizacji handlu narkotykami. Pojawiło się też podejrzenie, że zlecił mordestwo. Co prawda tego mu nie udowodniono, ale reszta oskarżeń wystarczyła, by sędzia skazał go na karę podwójnego dożywotniego pozbawienia wolności plus dodatkowe czterdzieści lat odsiadki, i to bez możliwości skrócenia kary. Surowy wyrok w zestawieniu z młodym wiekiem, doświadczeniem akademickim i prospołeczną, choć libertariańską postawą Ulbrichta, wywołał liczne protesty. Historia Ulbrichta to temat wielu artykułów, esejów, filmów dokumentalnych i kinowego thrillera *Wirtualne imperium* (oryginalny tytuł: *Silk Road*) z 2021 roku.

Wybierając giełdę, sprawdź…

1. czy giełda jest własnością publicznej firmy (notowanej na giełdzie)

2. czy giełda ma siedzibę w państwie o uznanym porządku prawnym; unikaj rajów podatkowych i republik bananowych

3. czy giełda oferuje zasilenie konta poprzez bezprowizyjne metody płatności; przelew kartą jest wygodny, ale prowizja może nas kosztować 5% środków

4. czy giełda umożliwia zabezpieczenie konta dwuetapową weryfikacją – jest to podstawa jakiejkolwiek aktywności w świecie kryptowalut; jeśli tak, to czy możemy zarejestrować w tym celu dwa klucze Yubi (są to przypominające pendrive'y narzędzia bezpieczeństwa – możemy nimi zabezpieczyć nie tylko konto giełdy, ale także większość istotnych serwisów, na przykład naszą pocztę elektroniczną; dwa klucze są potrzebne, by nie ryzykować utraty dostępu do konta w wypadku zgubienia jedynego zabezpieczenia)

5. politykę wypłat kont anonimowych oraz kont zarejestrowanych; pamiętaj, że wszystkie nieaktywne środki powinieneś przenieść na swój adres sprzętowy

Ograniczaj do niezbędnego minimum rozsyłanie skanów dowodu osobistego lub paszportu. W przypadku większych operacji na koncie będzie to nieuniknione. Zaletą jest możliwość dochodzenia naszych praw w przypadku problemów. Po włamaniu na giełdę Mt.Gox skradzione fundusze były zwracane właścicielom po okazaniu dokumentu użytego przy rejestracji konta. Korzystający z usług Mt.Gox zawdzięczają ten zwrot szczęśliwemu zbiegowi okoliczności – śledztwo trwało tak długo, że wartość tych nielicznych monet, które udało się odzyskać, wzrosła na tyle, że umożliwiła pokrycie strat!

Największe hacki kryptowalutowe w historii (za BBC):

611 milionów dolarów – Poly Network, styczeń 2021

540 milionów dolarów – Ronin Bridge, marzec 2022

532 milionów dolarów – Coincheck, styczeń 2018

470 milionów dolarów – Mt.Gox, luty 2014

325 milionów dolarów – Wormhole, luty 2022

6

Smartcity

– Cześć! Widziałem, że korzystacie z Kasią z tej nowej wypożyczalni w kampusie… Ale tam trzeba płacić tymi całymi tokenami, trochę bez sensu…

– E, nie… To bardzo wygodne! W dodatku daje więcej możliwości niż tylko korzystanie z wypożyczalni.

– Serio? A w czym to jest niby lepsze od normalnej karty albo płatności zegarkiem?

– Wypożyczalnia to nowoczesna firma. By rozpocząć działalność biznesową, stworzyła najpierw swoją kryptowalutę i odniosła sukces na giełdzie. Następnie zaproponowała naszej uczelni, by ta uczyniła ją swoim wewnętrznym środkiem płatności, bo to otworzy wiele możliwości. No i uczelnia się na to zgodziła. I chyba jest zadowolona.

– Tak? A co w tym takiego wspaniałego?

– Z punktu widzenia samej wypożyczalni dzięki kryptowalucie można lepiej zorganizować całe przedsięwzięcie. A z punktu widzenia studenta: posługując się swoim portfelem, jesteś w dużym stopniu anonimowy. Bez rezygnowania z prywatności możesz łatwo udowodnić, że mieszkasz w akademiku w kampusie, co daje ci zniżkę na wypożyczanie rowerów i innego sprzętu. W wypożyczalni dzięki transakcjom kryptowalutowym wiedzą na przykład, z którego akademika pochodzi najwięcej chętnych, który obszar kampusu najczęściej wypożycza rowery; tego typu rzeczy. Statystycznie, bez konieczności ujawniania tożsamości wypożyczających. Dzięki temu wypożyczalnia może zoptymalizować swoje działanie.

– No dobra, to jest dobre głównie dla nich, bo mogą się trochę lepiej zorganizować, ale co jeszcze my z tego mamy?

– Po tym, jak kryptowaluta wypożyczalni stała się wewnętrzną walutą uczelni, część stypendium można było na życzenie dostać w tokenach i wygodnie wykorzystywać w różnych wewnętrznych usługach. Na przykład obiady na stołówce opłacane tokenami kupujesz wówczas ze zniżką. Jeśli zgłosisz się do pomocy przy organizacji uczelnianych eventów, zarabiasz tokeny. To jeszcze nie wszystko. Możesz pokazać tym sposobem swoją aktywność. Jest też sporo bonusów za płatności tokenami, i to nie tylko takich, jak ten „stołówkowy": otrzymujesz zniżki, ale zyskujesz też pierwszeństwo, gdy chcesz skorzystać z jakiejś usługi, wynająć salę i tak dalej.

– Hm, brzmi całkiem nieźle!

Inteligentne miasto

Smartcity. To nie tylko jeden z wielu pomysłów na lepszą organizację życia w niewielkich społecznościach, takich jak miasteczka studenckie, dzielnice czy gminy. To idea znacznie głębsza i donioślejsza. Nowoczesne miasto może dysponować niesamowicie wydajną wirtualną infrastrukturą łączącą najważniejsze miejskie tkanki. A wszystko dzięki kryptowalutom i blockchainowi. No i Satoshiemu Nakamoto…

Myślę, że to, jak kryptowaluta i blockchain może usprawnić życie obywateli i wydajniej skomunikować ich z urzędami, usługodawcami i sprzedawcami, najlepiej omówić na przykładach. Wtedy o wiele bardziej namacalne staną się zalety kryptowalutowego smartcity.

Przede wszystkim przyjmijmy, że na jednej platformie obsługujemy zarówno infrastrukturę, jak i tożsamość mieszkańca miasta. I że ta tożsamość ujawniana jest tylko na moment, do potwierdzenia danych, a przez resztę czasu – w publicznej bazie danych, z której mogą korzystać

analitycy urzędów i usługodawców – użytkownik jest całkowicie anonimowy.

Mieszkanie, prąd, samochód

Rozważmy taki przykład. Nowe mieszkanie, którego adres jest zarządzany w blockchainie, zostało sprzedane. Jego nabywca, którego tożsamość też tkwi w blockchainie, poświadcza, że jest gotów płacić rachunki za prąd. Firma energetyczna włącza zatem prąd w tym konkretnym mieszkaniu (oczywiście zdalnie, sieciowo, za pośrednictwem blockchaina), nie wiedząc, kim jest w rzeczywistości jego lokator. Po prostu wiadomo, że w danym mieszkaniu będą opłacane rachunki. A ponieważ cały blockchain to platforma o rdzennie finansowym charakterze, opłaty również mogą odbywać się za jego pośrednictwem. Z zewnątrz widać tylko odpowiednie połączenia (adres mieszkania ma włączoną opcję odbioru prądu) i zużycie energii elektrycznej. Jej dostawca może zatem analizować zapotrzebowanie na nią i planować rozwój sieci, korzystając z dużej ilości anonimowych danych.

Unikalne połączenie jawności działań i anonimowości tych, którzy je podejmują, otwiera nowe możliwości usprawnienia życia w mieście.

Kolejny przykład: masz samochód, a mimo to decydujesz się skorzystać z komunikacji miejskiej. Przy zakupie biletu na autobus automatycznie nalicza ci się rabat. Miło! Twój zarejestrowany samochód jest widoczny w blockchainie i przypisany do twojej tożsamości (taki wpis powstał z chwilą jego kupna). To żaden problem wprowadzić taką automatyczną proekologiczną zachętę. Przypomnę tylko, że twoja tożsamość w blockchainie to jedynie długi ciąg losowych znaków. Nikt nie wie, że to

właśnie ty się za nim kryjesz. System widzi jednak, że do tego ciągu przypisano samochód, i udziela ci rabatu za każdym razem, kiedy wybierasz się na spotkanie ze znajomymi autobusem – dzięki takiemu rozwiązaniu można efektywnie zmniejszyć korki, zanieczyszczenie i emisję dwutlenku węgla. Dodatkowym bonusem wynikającym z tego, że nie prowadzisz samochodu, jest możliwość wypicia czegoś mocniejszego na miejscu, ale tego już nie zawdzięczasz bezpośrednio blockchainowi. Choć może trochę tak…

Możliwości takich powiązań są praktycznie nieograniczone. Przyjrzyjmy się temu, kontynuując naszą samochodową opowieść. Jeśli ładujemy samochód elektryczny, zapłacimy mniej za kilowatogodzinę energii elektrycznej. Rabat może się jeszcze zwiększyć, kiedy ładowanie przebiega w czasie nadprodukcji prądu. Pojemność baterii samochodów elektrycznych zwykle przekracza dzienne zużycie związane z jazdą po mieście, mogą więc stać się one magazynem energii na godziny wieczorne, gdy zapotrzebowanie na prąd jest większe, a odnawialne źródła, takie jak panele fotowoltaiczne, już go nie generują. Dzięki połączeniu wielu systemów możemy bardzo usprawnić życie w zatłoczonych miastach.

Warto zauważyć, że w infrastrukturze zasilania opartej na energii odnawialnej samochody elektryczne mają kapitalne – można rzec: centralne – znacznie. Stanowią magazyny energii, które niejako przemieszczają się w czasie i w przestrzeni: w czasie, kiedy energia jest przenoszona z godzin nadprodukcji na godziny zwiększonego popytu na prąd; w przestrzeni, kiedy pozostawiony na miejskim parkingu samochód przejmuje rolę punktu ładowania dla osób, które potrzebują „zatankować” prąd. Oczywiście wszelkie rozliczenia dokonują się za pośrednictwem zdecentralizowanej kryptowaluty. Zdecentralizowanej podobnie jak samochody… Protokół portfela we wtyczce twojego kabla do ładowania

zapłaci dokładnie za tyle energii, ile jej pobierzesz do czasu odjazdu sąsiedniego samochodu lub do limitu ustalonego przez jego właściciela. Być może ów właściciel okaże się na tyle uprzejmy, że przed odjazdem przepnie twój kabel do innego samochodu obok?

Za skompletowanie dziennego kombo: pozostawienie samochodu na podmiejskim parkingu typu park & ride, podzielenie się na nim nadwyżką energii, skorzystanie z publicznego transportu, by dojechać do centrum, i przejście pieszo dzielących cię od celu ostatnich pięciuset metrów – poza standardową obniżką opłaty parkingowej i rabatem na bilet autobusowy – możesz otrzymać dodatkowe punkty zmniejszające cenę ubezpieczenia zdrowotnego. A wszystko to jest zupełnie anonimowe! Blockchain umożliwia potwierdzanie wszelkich działań bez ujawniania tożsamości osoby, która ich dokonuje – dzięki kryptografii.

Co jeszcze potrafi blockchain obsługujący inteligentne miasto? System motywacji, ulg i bonusów, może również usprawnić przejazd przez aglomerację – wystarczy go tylko sprząc z nawigacją. Kierowca po ustawieniu celu podróży oprócz najkrótszej lub najszybszej trasy może otrzymać propozycje alternatywnych objazdów, zmniejszających korki w zatłoczonych w danej chwili obszarach miasta. Kierowca za zgodę na przejazd mniej korzystną dla niego trasą, ale za to korzystną dla ruchu w mieście, otrzyma wynagradzające bonusy.

Podobnie można wpływać na styl jazdy kierowców. W samochodach hybrydowych przy spokojnej jeździe wykorzystywany jest silnik elektryczny. Gwałtowniejsze przyspieszenia powodują uruchomienie silnika spalinowego. Można więc wprowadzić dodatkowe rabaty na prąd dla kierowców jeżdżących spokojniej, co ograniczy hałas, spalanie i zwiększy bezpieczeństwo w ruchu drogowym. Dzięki finansowemu

charakterowi blockchaina takie proekologiczne zachęty mogą być bardzo łatwo wdrożone.

Każdy samochód – niezależnie od tego, czy jest własnością firmy, czy osoby fizycznej – może za zgodą właściciela być udostępniany w programie carsharingowym. Lokalizacja samochodu, stawka za wypożyczenie, opłaty za ładowanie i użyczanie energii, wszelkie podziały kosztów eksploatacji i zysków ze współdzielenia między właścicielem i wypożyczającym odbywają się w czasie rzeczywistym, bez żmudnych bankowych rozliczeń, przelewów i blokad kwot na karcie, za to z uwzględnieniem wszelkich bonusów i zachęt, usprawniających życie i działających z korzyścią dla całego społeczeństwa.

Ekonomia „na zachętę” i piętnaście minut

Może się nam wydawać, że wiele z tych rozwiązań już działa (jak choćby ocenianie stylu jazdy kierowcy w systemach carsharingowych, co ma podnosić poziom bezpieczeństwa i zapobiegać nadmiernemu zużyciu samochodów), a reszta mogłaby zostać zrealizowana z wykorzystaniem istniejących już systemów informatycznych. Jednak w praktyce bez jednolitej platformy, zapewniającej spójne i ustandaryzowane zasady komunikacji, zintegrowane działanie tak wielu i tak różnorodnych miejskich mechanizmów będzie pozostawiało wiele do życzenia. Cykle życia niezależnych systemów często się nie zazębiają, a komunikacja między nimi stale zawodzi. Wprowadzanie coraz to nowych bonusów i zachęt w architekturze opartej na zwykłych pieniądzach zwiększa obciążenie prawne i wymaga zaufania do poszczególnych podsystemów.

Tymczasem jednolity blockchain tworzy swoją wewnętrzną, samowystarczalną ekonomię. Bez banków, kont, pośredników. W całej szeroko pojętej idei blockchainowego inteligentnego miasta nie chodzi tylko o to, żeby zużyć mniej benzyny i zaoszczędzić parę groszy na spokojnej jeździe hybrydą. Poprzez połączenie wszystkich pomysłów optymalizujących nasze życie w jeden ekosystem sięgamy głębiej, ku ważniejszym celom: chcemy jeździć spokojniej, by było bezpieczniej, chcemy jeździć w sposób przewidywalny, żeby starać się jak najszybciej odejść od paliw kopalnych.

Transparentność gromadzonych danych i możliwość ich analizy – z pełnym poszanowaniem prywatności użytkowników, którzy je generują – może wydatnie wspomóc procesy urbanizacyjne. Skuteczność zachęt może wpłynąć nawet na planowanie zabudowy dzielnic czy przebudowy miast. Dysponując obszernymi danymi – podkreślę to po raz kolejny: anonimowymi – i potężnymi narzędziami do ich analizy, możemy odkryć wzorce i schematy przemieszczania się mieszkańców, a następnie wprowadzać ulgi podatkowe i inne preferencyjne warunki dla sklepów lub zakładów pracy, których lokalizacja i dostępność ograniczyłyby ruch w mieście.

Istnieje już zresztą bardzo ciekawa koncepcja w tym duchu – mowa o „piętnastominutowych miastach”. Jest to pomysł takiego rozwoju miast, by większość potrzebnej mieszkańcom infrastruktury (sklepy, punkty usługowe, przychodnie, szkoły, restauracje i miejsca rozrywki) znajdowała się w zasięgu piętnastominutowego spaceru.

AirBnB, Uber – to przykłady ekonomii „na żądanie”. Blockchain otwiera nową erę ekonomii, i kto wie, czy nie skuteczniejszej: to ekonomia „na zachętę”.

Utopia czy dystopia?

Wspólna platforma technologiczna ujednolica standardy i ułatwia podłączenie do systemu czujników, detektorów i innych urządzeń miejskiego monitoringu, a wspólna platforma finansowa zachęca natychmiastowymi bonusami do działań, dzięki którym życie każdego z nas z dnia na dzień staje się łatwiejsze. Przemieszczamy się tak, by nie prowadzić do powstawania korków, wyrzucamy śmieci do pustych koszy, zamiast wciskać odpady do przepełnionych pojemników, wykorzystujemy prąd z sieci, kiedy dochodzi do jego nadprodukcji, a użyczamy go z akumulatorów w godzinach niedoboru energetycznego. Wspólna platforma jest otwarta dla każdego: zarówno dla osób fizycznych, jak i firm. Ułatwia optymalizację naszych zachowań, umożliwia także realizację etycznych działań, które lokalna społeczność chce wspierać, jak choćby kupowanie produktów spożywczych i kosmetycznych, których okres ważności zbliża się do końca. I najważniejsze: wszystkie wspomniane działania, tak pożądane społecznie i tak korzystne z indywidualnego punktu widzenia (oszczędność, komfort, spokój), w mieście z infrastrukturą opartą na blockchainie są wywoływane zachętą, a nie nakazem. To wielka zaleta systemu, bo zachęta jest o wiele skuteczniejsza niż nakaz.

Z technologicznego punktu widzenia zaletą blockchaina zaprzęgniętego do obsługi inteligentnego miasta jest – znów – jego decentralizacja. Zwykle serwisy dostarczane przez prywatne firmy działają na centralnych serwerach i polegają na ich nieprzerywanej awariami dostępności. Tymczasem blockchain opiera się na sieci równych sobie węzłów, jest zatem wyjątkowo odporny na przeciążenia i awarie. Jeśli jednak platforma blockchaina z jakichś powodów nie jest chwilowo osiągalna po stronie użytkownika (na przykład z powodu braku zasięgu), zawsze może on

zarejestrować dowolną akcję offline i pozostawić do wysłania w późniejszym czasie. Kryptograficzny podpis zapewni nienaruszalność, autentyczność i anonimowość jego wiadomości.

Smartcity. Utopia czy dystopia? Pełna kontrola nad obywatelami w stylu chińskiego systemu punktacji społecznej, tak świetnie pokazanego w odcinku *Na łeb, na szyję* serialu *Czarne lustro*? A może próba pchnięcia ewolucji miast na ścieżkę harmonijnego rozwoju?

Osobiście uważam, że nowoczesne państwa będą zmierzać ku w pełni zintegrowanym systemom kontroli, i to być może nawet ze słusznych pobudek. Ale bez systemu z blockchainem jesteśmy zdani na łaskę tego centralnego – uzależniamy od niego wypracowane zyski i tracimy prywatność. Subtelną różnicą jest to, że blockchain pozwoli budować inteligentne miasta dzięki oddolnemu ruchowi, na własnych zasadach; społeczności nie będą już musiały ulegać jakimkolwiek odgórnie narzuconym koncepcjom.

Samochód w centrum

W tym rozdziale wspomniałem o centralnym znaczeniu samochodu elektrycznego jako źródła energii w inteligentnym mieście. Więcej na ten temat można się dowiedzieć z artykułów na temat technologii V2L (*vehicle to load*), V2H (*vehicle to home*) lub V2G (*vehicle to grid*).

7

Ekologia

– Wiesz… Rozumiem zalety korzystania z blockchaina. Tyle że ostatnio usłyszałem, że to bardzo nieekologiczne. Górnicy zużywają gigantyczne ilości prądu, a sprzęt, który ciągle trzeba wymieniać na nowy, tworzy hałdy elektrośmieci…

– Owszem, starsze kryptowaluty, takie jak bitcoin, korzystają z algorytmów *Proof of Work* i rzeczywiście potrzebują sporo prądu. Ale prawie wszystkie nowsze i dziś funkcjonujące systemy kryptowalutowe opierają się na architekturze *Proof of Stake*, która nie wymaga dodatkowego wkładu energetycznego. Zresztą kwestia bitcoina i jego prądożerności wcale nie jest tak oczywista, jak by się mogło wydawać…

Czy krypto jest eko?

Czy kryptowaluty przyczyniają się do degradacji środowiska naturalnego? A może przeciwnie – może kryptowaluty są ekologiczne?

Na początku oddzielmy bitcoina od reszty kryptowalut, co ułatwi nam rozważanie. I załóżmy, że z punktu widzenia ekologii najbardziej problematyczny – ze względu na swoją prądożerność – jest właśnie bitcoin, a nie kryptowaluty w ogóle. W samych kryptowalutach nie ma nic szczególnie odróżniającego je od „zwykłych” systemów czy urządzeń

komputerowych, takich jak konsole do gier i sieciowe odtwarzacze filmów. Kryptowaluty to nic innego jak kombinacja istniejącej technologii cyfrowej i nowinek kryptograficznych.

Bitcoin to jednak spory kawałek tortu. To czterdzieści procent rynku kryptowalut. I tak, rzeczywiście – bitcoin to górnicy, kopalnie i mnóstwo prądu. Druga co do wielkości kryptowaluta, o połowę mniejsze od bitcoina ethereum, też zaczęła swój żywot jako system z górnikami, czyli korzystający z algorytmów *Proof of Work* (Dowód Pracy), ale we wrześniu 2022 przemigrowała do proekologicznego rozwiązania, jakim są algorytmy *Proof of Stake* (Dowód Udziału; szerzej o tej metodzie piszę na stronie 150 i dalszych). Ethereum było jednocześnie prekursorem badań nad takimi rozwiązaniami i udostępniło je wszystkim innym zainteresowanym blockchainom. Razem te dwie największe kryptowaluty odpowiadają za sześćdziesiąt procent rynku.

Algorytmy *Proof of Work*, które stoją na straży bezpieczeństwa sieci kryptowalutowej, korzystają z tak zwanych koparek – ich zadaniem jest procesowanie bloków z zapisanymi transakcjami (omawialiśmy to w poprzednich rozdziałach). Koparką może być zwykły komputer, w praktyce jednak wymaganą moc obliczeniową są w stanie zapewnić wyłącznie specjalistyczne urządzenia. Ilość prądu zużywanego w procesie kopania przez koparki i ich operatorów – górników – do przeprowadzania wymaganych przez algorytmy obliczeń to faktycznie spory problem energetyczny. Nikogo nie trzeba przekonywać, jak ważna jest ekologia i konieczność oszczędzania wszelkich zasobów energii, nic więc dziwnego, że już sama skala systemów kryptowalutowych wywołuje do przysłowiowej tablicy zarówno ich twórców, jak i użytkowników.

Bitcoin a ekologia

Czyli… bitcoin jest nieekologiczny? Tylko marnuje energię? Przepala prąd? Rozczaruję i przeciwników, i zwolenników kryptowalut: obawiam się, że odpowiedź na to pytanie jest bardzo złożona. Powstało wiele raportów o energochłonności kryptowalut. Dokumenty te sporządziły rozmaite instytucje – organizacje ekologiczne, uczelnie, Bank Rozrachunków Międzynarodowych – które aktywnie monitorują problem zużycia prądu. Czytając owe raporty, z zaskoczeniem stwierdziłem, że prezentowane w nich wnioski są rozbieżne. Analizy objęły bowiem różne aspekty systemu kryptowalutowego – to ich największy mankament. Spójrzmy więc na te raporty krytycznym okiem. Wyróbmy sobie własne zdanie. A ostateczny werdykt pozostawmy naukowcom i ekspertom.

By jednak nabrać wprawy w ocenie, rozpatrzmy przykład, który już wcześniej w tej książce pomógł nam sporo zrozumieć. Mowa o samochodzie elektrycznym.

Zatem: czy samochody elektryczne są ekologiczne?

Ekologia elektromobilności

Rewolucja na rynku samochodów ekologicznych zaczęła się od Toyoty, a Toyota Prius to jedno z pierwszych aut hybrydowych. Model przełomowy, w szczególności jeśli chodzi o upowszechnienie napędu hybrydowego. Priusa produkowano wyłącznie w Japonii, a dużym rynkiem jego zbytu były Stany Zjednoczone.

Czy Prius to model ekologiczny? Zależy jak na to spojrzeć. Jeśli pod uwagę wziąć kurierów i taksówkarzy wykorzystujących zalety napędu

hybrydowego w jeździe miejskiej, to tak: Prius oszczędzał benzynę i emitował mniej spalin, co w zatłoczonych i często zakorkowanych aglomeracjach jest nie do przecenienia. Lecz przecież nie zawsze był eksploatowany w warunkach, w których ujawniały się korzyści z napędu hybrydowego. Jedna z pierwszych stosowanych w Priusie skrzyń biegów, przekazująca moc z silników elektrycznego i spalinowego do układu napędowego, nie była mistrzem wydajności. Samochód w jeździe pozamiejskiej często wchodził na wysokie obroty, a międzymiastowe przejazdy po autostradach były codziennością amerykańskich posiadaczy Priusa. Prius spalał wtedy więcej benzyny niż zwykły samochód spalinowy.

Skoro mowa o amerykańskich właścicielach: musimy przecież uwzględnić transport Priusa z Japonii do Stanów. Nie jest to mała odległość. Kontenerowce przewożące samochody spalają paliwo najgorszej jakości w silnikach, które mają po kilkadziesiąt lat.

W zależności od tego, czy do oceny ekologiczności Priusa wliczymy koszty jego transportu i utylizacji jego baterii oraz czy weźmiemy pod uwagę także warunki jego eksploatacji, otrzymamy skrajnie różne wyniki śladu węglowego generowanego przez ten samochód. Dopiero uwzględnienie wszystkich tych czynników pozwala wydać werdykt, czy Prius jest ekologiczny, czy nie.

Minęło niemal dwadzieścia lat od premiery pierwszego Priusa. Volvo opracowało w tym czasie rewelacyjną skrzynię biegów i coraz popularniejsze stały się hybrydy plug-in. Produkcja samochodów hybrydowych na całym świecie bardzo się upowszechniła, praktycznie zniknął problem kosztów dalekiego transportu. Jednak wraz z większymi bateriami stosowanymi w tych autach pojawiły inne dylematy. Jak ekologiczna jest ich produkcja z metali ziem rzadkich? Skąd bierze się prąd, który je ładuje? Z ogniw fotowoltaicznych? A może z elektrowni

węglowych? Pamiętajmy, że na początkowym etapie rozwoju hybryd plug-in szybkie ładowanie nie było jeszcze dostępne. Samochody musiały być ładowane w nocy, kiedy fotowoltaika nie działa. Gdy drastycznie spada pojemność baterii, musimy oczywiście ją zutylizować. Tu mam na szczęście dobre wieści: baterie w hybrydach dobrze się starzeją i z wiekiem nie wykazują dużych oznak zużycia. Pozostaje zatem rozwiązać problem samochodów najstarszych i powypadkowych.

I znów w zależności od tego, jakie aspekty uwzględnimy w naszej dyskusji o ekologii, dojdziemy albo do wniosku, że hybrydy plug-in jeżdżą na czystym prądzie, albo że są ekologicznym problemem na dziesięciolecia.

To jeszcze nie koniec naszej samochodowej opowieści. Niekwestionowanym prekursorem w pełni elektrycznych samochodów jest Tesla. Tesla produkuje samochody, które mają świetny zasięg i które można szybko naładować w miejscu oddalonym o sto kilometrów od największego skupiska odbiorców tych aut – miasteczek Doliny Krzemowej po drugiej stronie Zatoki. Tesla współpracuje z firmą zajmującą się fotowoltaiką i wspiera rozwój tej technologii (choćby poprzez wprowadzenie na rynek fotowoltaicznych dachówek). Samochody Tesli podłączone do szybkiej ładowarki uzupełniają energię w ciągu pół godziny – całonocne maratony przy gniazdku sieciowym już nie są jedyną opcją. Nadal jednak wzbudzają kontrowersje kwestie wydobycia metali potrzebnych do produkcji baterii i utylizacji zużytych akumulatorów.

Pozostaje jeszcze aspekt społeczny. Samochody elektryczne są znacznie prostsze w budowie od spalinowych. Fabryki montują je znacznie szybciej i mogą być bardziej zautomatyzowane niż fabryki produkujące tradycyjne samochody spalinowe. Pojawiają się głosy ze strony japońskiego przemysłu motoryzacyjnego, które świadczą o chęci wstrzymania bądź spowolnienia elektrycznej rewolucji w motoryzacji. Argumenty są wielostronne: od

porównywania „elektryków” z czystymi dalekozasięgowymi dieslami, po zwracanie uwagi na problemy społeczne, wynikające ze wzrostu bezrobocia w przemyśle motoryzacyjnym.

Intuicja podpowiada nam, że samochody elektryczne to nasza przyszłość. Postęp jest nieubłagany. Z każdym rokiem pozostaje coraz mniej problemów do rozwiązania; na przykład niedawno naukowcy opracowali metodę ekstrakcji litu z wody morskiej. Zanim jednak przejdziemy w pełni na elektromobilność, mogą upłynąć dziesięciolecia.

Przykład z samochodami miał pomóc unaocznić ci, że w zależności od tego, które aspekty weźmiemy pod uwagę i jak szeroko będziemy je analizować, możemy dojść do różnych wniosków.

Bitcoin pod energetyczną lupą

Obserwowałem historię bitcoina od samego początku, a aktywnie ją współtworzę od dobrych paru lat. Dyskusję o ekologii kryptowalut postrzegam trochę tak, jak powyższy przykład dyskusji o ekologii elektromobilności. Czasem wszystkie kryptowaluty wrzuca się do jednego worka, nie biorąc pod uwagę, że część z nich nie ma nic wspólnego z ponadnormatywnym zużyciem prądu. Innym razem dość wybiórczo ocenia się wpływ bitcoina na nasz świat.

Mam dla ciebie garść ciekawostek, sloganów, mitów. Zastanów się nad nimi i przekonaj się, co sam sądzisz o ekologii bitcoina i innych kryptowalut.

Zacznijmy od razu od zarzutów: prognoza zużycia prądu przez bitcoin do zabezpieczenia publicznej bazy danych to 200 TWh (terawatogodzin) rocznie! Ta nowa zabawka komputerowych geeków niepotrzebnie zużywa

aż tyle prądu! Jest to aż prawie 1% globalnej produkcji prądu. Jednak to tylko wartość szczytowa, rzeczywiste zużycie często bywa mniejsze; oczywiście w przeszłości było znacznie niższe. Z dużą dozą pewności można natomiast założyć, że w przyszłości nastąpi jego wzrost.

SLOGAN 1
Bitcoin zużywa tyle prądu co Tajlandia!

Dobrze znam ten slogan i tak, to prawda. W miarę upływu lat w haśle zmieniał się kraj. Gdy kiedyś usłyszałem, że bitcoin zużywa tyle prądu co Dania, byłem pozytywnie zaskoczony, przecież to malutki kraj, który ma wręcz obsesję na punkcie troski o ekologię. Nie mogło być lepiej! Już chyba rozumiesz, że stwierdzenia tego typu mają tylko wzbudzać kontrowersje. Wiesz, ile prądu zużywa Dania? A Tajlandia? Nawet jeśli znajdziemy tę statystyczną wartość w sieci, wciąż będzie tylko abstrakcyjną, nic niemówiącą liczbą. Musimy znaleźć jakieś lepsze porównanie. Istnieje, o czym poniżej.

Zużycie prądu przez bitcoin jest tego samego rzędu, co zużycie prądu systemu bankowego na całym świecie. To porównanie często ma na celu zdyskredytowanie bitcoina: prąd w jego przypadku jest zużywany na rozwiązywanie kryptozagadki, a w bankach na rzeczywiste operacje finansowe. Kryptozagadka to dla ciebie nic nowego – to tylko inna nazwa operacji z użyciem funkcji hashującej, którą porównałem do robienia koktajlu. Nie jest to żadna łamigłówka dla przyjemności, ale sposób na zabezpieczenie sieci bitcoina oraz zagwarantowanie jej nienaruszalności. Tymczasem gdy spojrzymy na system bankowy szerzej i weźmiemy pod uwagę liczbę jego pracowników, budynki oddziałów, ich wielkość i miks

energetyczny, z którego korzystają, emisja CO_2 bitcoina okazuje się dziesięciokrotnie mniejsza niż ta w sektorze bankowym.

Tak samo nie ma większego sensu porównywanie liczby transakcji w bitcoinie do liczby transakcji bankowych czy transakcji dokonywanych kartami Visa lub Mastercard. Transakcje bankowe reprezentują pojedynczą operację finansową. Gdy będzie ich więcej, będzie trzeba rozbudować systemy bankowe ze wszystkimi tego konsekwencjami, w tym większym zużyciem prądu. Transakcja w systemie bitcoina może być transferem finansowym, ale również może stanowić reprezentację dowolnego stanu rzeczy, na przykład zabezpieczenia stu tysięcy transakcji w innym systemie. Pojęcia „transakcja bankowa” i „transakcja kryptowalutowa” nie oznaczają tego samego. W banku transakcją będzie zawsze pojedynczy transfer środków, a w świecie kryptowalut to dowolna, niepodzielna i nienaruszalna operacja systemowa.

O transakcjach kryptowalutowych już zresztą pisałem i będę jeszcze pisał; ogólnie rzecz biorąc, to wszystkie zdarzenia rejestrowane w blockchainie (na przykład w rozdziale 8 omawiam „blockchainowe” wypożyczenie samochodu na lotnisku – transakcja w tym wypadku zawiera tak zwany Dowód Istnienia: zdjęcie samochodu dokumentujące niepodważalnie jego stan w danym czasie). Nic zatem nie stoi na przeszkodzie, by jedna bitcoinowa transakcja zawierała skrót wielu operacji, na przykład wszystkich zdarzeń zarejestrowanych w ciągu jednego dnia przez system automatyki budynkowej „inteligentnego” czterdziestopiętrowego biurowca. To miliony zdarzeń: otwarcie drzwi, zamknięcie drzwi, przyjazd windy, zwiększenie temperatury, otwarcie okna… Możemy sobie wyobrazić, że każdego dnia system biurowca tworzy tylko jedną transakcję w bitcoinie, reprezentującą miliony tych zmian stanu urządzeń i innych elementów budynku. Być może dzięki temu

ubezpieczenie nieruchomości stanie się tańsze. Dzięki bitcoinowi ubezpieczony będzie bowiem dysponował niekwestionowanym i nienaruszalnym dowodem, że okno zalanego pomieszczenia podczas zeszłotygodniowej nocnej nawałnicy było na pewno zamknięte.

A skoro już jesteśmy przy transakcjach…

SLOGAN 2
Jedna transakcja bitcoina potrzebuje milion razy więcej prądu niż transakcja bankowa!

Ten slogan wszystko wypacza! Przez takie świadome i zamierzone błędy rzeczowe trudno polemizować z argumentami porównującymi zużycie prądu przez jedną transakcję bankową i przez jedną transakcję w bitcoinowym blockchainie. To przecież dwie różne sprawy! Są zupełnie czymś innym!

Wiemy na pewno, że bitcoin zużywa mniej więcej tyle samo prądu co system bankowy, który jest oczywiście olbrzymi i nieporównywalnie szerzej stosowany. W porządku, pogódźmy się z tym. Mam jednak w zanadrzu szokujące porównanie, które przechyli szalę na stronę bitcoina. Otóż bitcoin zużywa tyle samo prądu, co 20% urządzeń w Stanach Zjednoczonych pozostawionych w trybie standby. Podkreślę: mowa tu o nieużywanych urządzeniach, które nie działają, ale oczekują na włączenie w trybie gotowości. Niech ten argument będzie swego rodzaju odważnikiem, który znacząco zwiększy wagę korzyści na rzecz nowego wynalazku: bitcoin kontra trywialne ułatwienie sobie życia w starym świecie poprzez niewyłączenie urządzeń.

A wspomniałem tylko o USA. Chiny zużywają dwukrotnie więcej prądu, przy czym te dwie gospodarki to niewiele mniej niż połowa ogólnoświatowej konsumpcji energii elektrycznej… Odważnik staje się coraz cięższy.

Zresztą podobnych przykładów jest wiele. Można dyskutować o energochłonności bitcoina w porównaniu do zapotrzebowania na prąd w przemyśle wydobywczym złota (bitcoin jest znacznie oszczędniejszy i przyjaźniejszy środowisku) lub choćby przemysłu rozrywkowego (tak – bitcoin zużywa mniej prądu niż globalna sieć gier wideo), ale nie o to przecież chodzi. Bitcoin zaproponował nową jakość: decentralizację. Zaoferował też w pełni publiczną, a przy tym anonimową bazę danych. Początkowo ceną tej jakości był prąd. Teraz – w miarę rozwoju ekosystemu kryptowalut – bitcoin staje się pomostem łączącym świat rzeczywisty z wirtualnym. Można też postrzegać go jako dźwignię promocyjną lub zabezpieczenie dla nowych, „lekkich” i mniej prądożernych systemów kryptowalutowych.

Wyczyny w ekologii – ASIC

A czy możemy odwrócić dyskusję? Zamiast upewniać się, że bitcoin może nie jest aż tak nieekologiczny, jak się powszechnie wydaje, zapytajmy, czy bitcoin w ogóle ma jakieś ekologiczne walory.

Owszem, ma, i jest ich wiele! Niestety, część z nich jakimś dziwnym trafem w ogóle nie pojawia się w raportach o wpływie bitcoina na środowisko.

Jestem człowiekiem, który siedzi po uszy w technologii, w szczególności technologii kryptowalutowej – dlatego zwracam uwagę na

wiele jej aspektów, które nie przedostają się do mainstreamu, tymczasem naprawdę warto o nich wiedzieć. I takim właśnie aspektem jest… usprawnienie projektowania urządzeń ASIC… Brzmi zbyt hermetycznie? Już wyjaśniam.

ASIC to akronim pojęcia *application-specific integrated circuit* – w języku polskim tłumaczymy je jako: „specjalizowany układ scalony". Najprościej rzecz ujmując, jest to komputer wykonujący tylko jedną konkretną rzecz, do której został zaprojektowany. Może być kasownikiem. Może analizować dane pochodzące z czujników w samochodzie. Może być częścią naszej domowej sieci wi-fi (w routerze). Takie specjalizowane komputery projektuje się wówczas, gdy w skali masowej pojawia się potrzeba konkretnej funkcjonalności. Aby wyprodukować ASIC, fabryka procesorów musi wdrożyć nowy projekt (albo powstać od nowa). Projekt jest zwykle skomplikowany, kosztowny, żmudny i zabiera dużo czasu – przeciętnie kilkanaście miesięcy. Bywa, że zanim dojdzie do sfinalizowania prac projektowych, zleceniodawca (albo rynek) traci zainteresowanie danym ASIC-iem. Przynajmniej tak było do niedawna.

I tu na scenę wkracza bitcoin. Algorytmy napędzające blockchain zapoczątkowały rewolucję w projektowaniu ASIC-ów. Jak pamiętasz, zabezpieczenie sieci Bitcoin (zatwierdzanie bloków z transakcjami) odbywa się w wyniku obliczeń wykorzystujących funkcję hashującą. To konkretna funkcjonalność. Idealna do zaimplementowania w zintegrowanym układzie scalonym, który będzie realizował tylko ją i działał optymalnie.

Dzięki bitcoinowi rozpoczął się prawdziwy wyścig zbrojeń. Wiele firm, w szczególności z południowo-wschodniej Azji, zainwestowało wielkie środki, by usprawnić proces projektowania i produkcji coraz to szybszych układów zintegrowanych typu ASIC. Dlaczego? Optymalizacja energetyczno-wydajnościowa ASIC-ów to szybsze znalezienie ciągu

z kilkunastoma zerami, który zatwierdza blok, i większe prawdopodobieństwo otrzymania bitcoinowej wypłaty!

Główny postęp w projektowaniu ASIC-ów dokonał się na specyficznym odcinku kryptowalutowym, ale beneficjentem tego ulepszenia są pozostałe gałęzie przemysłu.

O jakich korzyściach mowa? Na przykład czas projektowania ASIC-ów uległ skróceniu z miesięcy do… tygodni! Fabryki zaś stały się bardziej elastyczne, a koszty budowy nowych linii produkcyjnych znacznie spadły.

Dzięki temu próg zastosowania specjalizowanych układów zintegrowanych jest znacznie niższy. To bardzo dobrze: zużywają one znacznie mniej prądu niż uniwersalne procesory, między innymi do chłodzenia, bo nie nagrzewają się tak mocno. Do ich produkcji potrzeba mniej materiałów, a w ostatnich cyklach życia generują mniej odpadów. Z owoców tego postępu będziemy korzystać przez nadchodzące dziesięciolecia – postępu, który był możliwy dzięki inwestycjom w nową dochodową technologię: kryptowaluty.

Wytwarzanie i przesyłanie prądu

Przenikanie się wyrafinowanej technologii z czymś tak pozornie mało wyrafinowanym jak prąd elektryczny jest bardzo ciekawe. W końcu to energia elektryczna jest paliwem napędzającym cały nasz świat cudów technologicznych. Również i w tej dziedzinie bitcoin odegrał znaczącą rolę. Tak jak zachęcił projektantów urządzeń do inwestycji w optymalizację (czasową i kosztową) procesu projektowania i wytwarzania układów zintegrowanych ASIC, tak ogólnie stymuluje usprawnianie odnawialnych

źródeł energii (OZE). Więcej: często również umożliwia używanie odnawialnych źródeł energii…

Z OZE jest pewien problem: w wielu przypadkach znajdują się one tam, gdzie nie ma ludzi… Jak więc rozwiązać kwestię pobierania z nich prądu? Wiadomo – trzeba budować energetyczne linie przesyłowe. Płynie w nich prąd o bardzo wysokim napięciu – ze względu na jego spadek wraz z długością kabla. Napięcie na typowej międzymiastowej linii przesyłowej wynosi od stu do trzystu tysięcy woltów. Odległości, na których straty (i wynikający z nich spadek napięcia) są na akceptowalnym poziomie, to setki kilometrów. Co jednak, jeśli elektrownia wodna jest oddalona od odbiorców energii o dwa tysiące kilometrów? Albo o pięć tysięcy? Takie sytuacje zdarzają się nie tylko w Azji, ale także w wielu innych miejscach na Ziemi – tam, gdzie ludzie osiedlają się na wybrzeżach, a energię produkuje się na odległym od nich obszarze, na którym istnieją korzystne warunki (fizyczne i ekonomiczne) do budowy elektrowni wodnych lub słonecznych.

I właśnie dlatego czasem bywa tak, że elektrownia jest na pustkowiu – z dala od wielkich miejskich aglomeracji – bo powstaje głównie z myślą o zasilaniu fabryk w jej bliskim sąsiedztwie. Co jednak, gdy przemysł ciężki przeprowadza się w inne miejsce lub kończy swoją działalność ze względu na brak zapotrzebowania na jego produkty? Co można zrobić z taką starą elektrownią, która straciła odbiorcę prądu? Praktycznie nic. Stoi zatem przez lata, eksploatowana w minimalnym stopniu… Może powinna powstać linia przesyłowa? Jest to jakiś pomysł, ale nie zawsze opłacalny. Budowa długiej wysokonapięciowej linii przesyłowej to złożona inwestycja z wieloma potencjalnymi problemami do rozwiązania. Dewastacja środowiska to jeden z nich – im większe jest napięcie, tym większe wymagane są odległości między przewodami a otoczeniem; niebezpieczne

łuki elektryczne, wywołujące pożary lasów, to kolejny kłopot. Tymczasem dzięki bitcoinowi stare elektrownie odżyły. Utylizują prąd na miejscu. Ten sposób ich wykorzystania nie tylko zrewitalizował pośrednio wiele regionów, które nie miały perspektyw na żadne inwestycje, ale także skierował nowe środki na ulepszanie elektrowni. W rezultacie dokonuje się tu kolejny postęp! Zoptymalizowane przez stymulację bitcoinem projekty elektrowni OZE mają szansę nie tylko na przetrwanie, ale i na rozwój!

Widać tu analogię do ewolucji pieniądza, którego reprezentacja z biegiem czasu się zmieniała i po zupełnie fizycznych zyskiwała coraz bardziej abstrakcyjne formy wartości: od płodów rolnych, przez metale szlachetne, po zapis elektroniczny. Wydajne transportowanie energii również trafiło na podobną ścieżkę ewolucji. Jednym z jej etapów była… produkcja aluminium. Odbywała się w rejonach świata z tanią energią elektryczną, takich jak Islandia (tani prąd Islandczycy otrzymują z zaprzęgnięcia do jego generowania aktywności wulkanicznej swojej wyspy). Gotowy produkt był do odbiorców transportowany statkami. W tym wypadku transport energii elektrycznej przeistoczył się w wydajniejszą formę niż przesyłanie elektronów. Bitcoin to kolejny etap tych zmian.

Scenariusze nieco bardziej odległe w czasie, graniczące już z fantastyką naukową, choć może wcale nie, opisują zastosowanie kryptowalut w recyklingu technologii odnawialnych. Mało wydajne – ze względu na wiek technologii lub zużycie – panele fotowoltaiczne muszą być zastępowane ich nowymi generacjami. Stare panele nie za bardzo jest gdzie umieścić – przestrzeń w miastach i poza miastami staje się coraz bardziej cenna i ograniczona. Niechciane panele mogłyby zatem posłużyć do zbudowania sztucznej solarnej wyspy gdzieś na oceanie: wyspy zasilającej sieć kryptowalutową. Nie dość, że takie rozwiązanie rozprawia się

z kwestią fotowoltaicznych elektrośmieci, to jeszcze samo się finansuje! Bez bitcoina coś podobnego nie byłoby do pomyślenia.

No dobra, wróćmy z przyszłości do teraźniejszości. Zupełnie niewyimaginowanym problemem, z którym borykamy się obecnie, jest obciążenie starej infrastruktury sieci energetycznych przez nowe metody generowania prądu. W Polsce za przeważającą część produkcji prądu odpowiada kilkadziesiąt elektrociepłowni. Wdrażane w kraju programy ekologiczne promują model rozproszony, oparty na przydomowych elektrowniach fotowoltaicznych. Powoduje to realny problem nadprodukcji energii w dzień i jej niedoboru w nocy. Ponieważ bitcoin to moja codzienność, oczywistym wydaje mi się dołożenie elementu w postaci kryptowalutowej technologii do reszty energetycznej układanki. Moglibyśmy wyposażyć przydomowe elektrownie w koparki bitcoina i zarządzać ich zasilaniem na poziomie powiatu lub województwa. Jeśli fotowoltaiczna nadprodukcja prądu zmuszałaby elektrociepłownie do niekorzystnej i kosztownej rekonfiguracji, można by zdalnie włączać koparki i odbierać tę nadwyżkę energii u źródła, unikając w ten sposób destabilizacji sieci.

Zresztą podobne rozwiązanie już istnieje! Niektórzy korzystają z koparek zintegrowanych z domowymi systemami ogrzewającymi wodę – woda w zasobnikach odbiera ciepło generowane w procesie kopania! I choć tego typu rozwiązania są na razie dziełem fascynatów nowinek technologicznych i majsterkowiczów, niewykluczone, że mogą trafić pod strzechy. Zresztą chyba sam dostrzegasz tu pewne podobieństwo do usprawnień technologicznych, które przedstawiłem w rozdziale „Smartcity”.

Opisałem tam samochody elektryczne jako mobilne baterie, które mogą przyjmować i oddawać prąd, gdy zachodzi taka potrzeba. Wróćmy na

chwilę do tego pomysłu. Rozwiązuje on bowiem w dużej mierze problem dostępności ładowarek i usuwa największą przeszkodę w rozwoju elektromobilności. Połączenie w tym samym miejscu i czasie dostępności środka rozliczeniowego (kryptowaluty) z dostępnością obiektu, którego dotyczy transakcja (samochód elektryczny), bardzo stymuluje rynek. Oto możemy zastąpić stacje ładowania innymi samochodami, które dysponują nadwyżką energetyczną. Mieszkający na przedmieściach użytkownicy samochodów elektrycznych mogą je codziennie ładować do poziomu powyżej koniecznego do odbycia podróży w tę i z powrotem. W czasie postoju, kiedy oni są w pracy, ich samochód może dosłownie sprzedawać nadwyżkę po dobrych cenach! Podwójny zysk!

Żeby wszystkie takie optymalizacje mogły działać – z olbrzymią korzyścią dla środowiska naturalnego – potrzeba długoterminowej, przemyślanej strategii, która zainspiruje inżynierów i producentów do zaprojektowania i zbudowania trwałych, bezawaryjnych urządzeń działających we wszystkich wspomnianych schematach współzależności.

Wspaniałą synergię kryptowalutowych algorytmów Dowodu Pracy z przemysłem możemy zauważyć w wielu innych zaskakujących sytuacjach. Weźmy skandynawski przemysł drzewny… W Norwegii działa centrum danych i kopalnia bitcoina KryptoVault. Korzysta wyłącznie z odnawialnych źródeł energii. Ale co to ma wspólnego z drzewami? Otóż całe odpadowe ciepło generowane przez koparki kryptowalutowe jest używane do osuszania drewnianych kłód!

Norwegia chlubi się bardzo ekologicznym miksem energetycznym, w którym energia elektryczna w 92% jest generowana przez elektrownie wodne, a w 6,4% przez elektrownie wiatrowe. Bitcoin to dla Norwegów sposób na rozwój północnych regionów kraju – znajduje się tam jeszcze więcej zasobów wodnych do wykorzystania. Już teraz ten kraj o niewielkiej

przecież populacji (5,4 miliona) ma jednoprocentowy udział w kopaniu bitcoina. Co więcej, norweski bitcoin jest stuprocentowo czysty!

Monety czyste i brudne

I tak oto dochodzimy do kolejnego bardzo ciekawego (i ekologicznego) aspektu bitcoina. Jego publiczna baza danych – blockchain – oprócz tego, że zapisuje wszelkie transakcje, księguje także nagrody przyznane górnikom za zatwierdzanie bloków. To z tej nagrody górnik finansuje koszt kopania (oczywiście jej część to też dochód górnika). Co ważne: wpis do blockchaina o nagrodzie dla górnika zawiera również informację o tym, czy dana moneta pochodzi z odnawialnych źródeł energii, czy z tradycyjnych! Dzięki temu – jako osoby, którym ochrona środowiska bardzo leży na sercu – możemy zadeklarować chęć używania wyłącznie ekologicznych bitcoinów. Pozwala na to coraz więcej aplikacji.

Takich ekologicznych monet jest naprawdę dużo. Szacuje się, że od 45% do 75% miesięcznie – w zależności od pory roku i liczby górników – pochodzi z odnawialnych źródeł energii!

Często powtarzanym mitem jest to, że kryptowaluty konkurują o odnawialną energię z ludźmi. Chyba już widzisz, że to… mit. Tam, gdzie odnawialna energia jest łatwo dostępna i tania, tam niestety nie mieszkają ludzie.

Skoro udział ekologicznych bitcoinów w ich całkowitej produkcji waha się między 45% a 75%, to skąd pochodzą pozostałe? Wydawać by się mogło, że na pewno z najtańszych źródeł. Oczywiście – jak wynika z rozkładu górników bitcoina na mapie świata – pochodzenie „brudnych” bitcoinów koreluje z terenami, na którym działają producenci taniego węgla

i taniej ropy. Iran, Kazachstan, Malezja. Ale to nie jedyny aspekt – nie zawsze stamtąd pochodzi najwięcej nieekologicznych monet: rządy takich państw nie zawsze są przychylne górnikom i często zakazują kopania. Powody są dwa. Pierwszy jest techniczny: pobieranie dużej mocy ze słabowitych sieci energetycznych może prowadzić do ich przeciążenia. Drugi jest polityczny: kryptowaluty pozwalają stworzyć alternatywną ekonomię, wymykającą się spod kontroli lokalnych reżimów.

Inne źródła „brudnych” bitcoinów mogą powstawać tam, gdzie pojawiają się zachęty do kopania przy nadwyżkach energii. Wśród górników nieekologicznych monet pojawiają się też, co zaskakujące, „drogie” miejsca, takie jak Niemcy czy Irlandia. To z kolei można wyjaśnić chęcią jak najtańszego kopania w jak najstabilniejszych prawnie państwach, gdzie nie ma ryzyka utraty sprzętu i innych zagrożeń natury prawnej – to bardzo ważne aspekty administrowania kopalniami bitcoinów. Podsumowując: sieć górników jest bardzo dobrze rozproszona w skali globu, a wydobycie „brudnych” bitcoinów nie pokrywa się geograficznie w stu procentach z producentami brudnej energii.

Musimy też pamiętać, żeby nie przeliczać ślepo zużywanego prądu na emisję dwutlenku węgla za pomocą jednego uśrednionego przelicznika. Jedna megawatogodzina z hydroelektrowni to emisja dziesięciu kilogramów CO_2. Ta sama ilość energii z elektrowni na paliwa kopalne to aż tysiąc kilogramów CO_2. Zważywszy na spory udział źródeł odnawialnych w wydobyciu monet kryptowalutowych, trudno nie przyznać, że bitcoin staje się jeszcze bardziej ekologiczny!

Ekologia to jednak nie tylko dwutlenek węgla i jego cieplarniane ekwiwalenty. Zwróćmy uwagę, że bitcoin (na razie) wytwarza mniej CO_2 niż przemysł wydobycia złota. Co ważniejsze, cyfrowe złoto – jak się często mówi o bitcoinie – negatywny wpływ na środowisko ogranicza tylko

do emisji CO_2. Tymczasem przemysł wydobycia złota to głęboka dewastacja środowiska, przekopanie kilometrów sześciennych ziemi i zastosowanie toksycznych chemikaliów do pozyskania ostatecznej formy metalu. Pamiętaj o tym, gdy ktoś będzie chciał cię przekonać do swoich racji za pomocą jednej liczby. Jeśli chcesz dowiedzieć się więcej, zapoznaj się z pracami Hassa McCooka – znajdziesz tam mnóstwo fascynujących komentarzy i danych związanych z dyskutowanymi tu tematami.

Jeszcze jeden przykład

Hm, miałem już przestać sypać przykładami, ale kusi mnie, by podać jeszcze jeden. A więc tak: elementem procesu wydobycia ropy naftowej – i to takim rzucającym się w oczy – są flary gazowe (zwane także świeczkami lub pochodniami). Ten płonący nad rafinerią bądź placem wiertniczym płomień gazowy to sposób na opróżnienie instalacji z gazu ziemnego, który pojawia się przy wydobyciu ropy lub przy procesach przetwarzania węglowodorów. Dzięki temu spalamy gaz, którego nie możemy magazynować ze względu na opłacalność ani przesyłać do odbiorców, bo nie dysponujemy instalacją przesyłową (gazociągiem). Ze względu na bezpieczeństwo musimy się gazu pozbyć, więc go spalamy. Jest to proces marnotrawiący duże ilości energii oraz bardzo zanieczyszczający środowisko… Idealnie nadaje się natomiast do zasilenia lokalnej kopalni bitcoina! Opłaca się to nawet w tak drogich rejonach świata jak Teksas, gdzie koparki w przenośnych kontenerach redukują o ponad 60% dwutlenek węgla emitowany przez flary i przynoszą zyski operatorom.

Powyższy przykład znakomicie unaocznia, że bitcoin wraz ze swoim blockchainem wcale nie potrzebuje sieci elektrycznej i prądu – potrzebuje

po prostu energii, w dowolnej postaci!

A teraz domknięcie cyklu: za pomocą układów ASIC (których wytwarzanie zoptymalizował bitcoin) możemy podłączyć się pod wszelkie źródła marnotrawionej energii, jak hamujący samochód, nadmiarowe przepalanie paliw kopalnych i wiele innych.

Nie znam się, ale się wypowiem

Zróbmy jeszcze krok wstecz. Pozwoli nam to poszerzyć spojrzenie na ekologię i problem zużycia prądu. Chciałbym przytoczyć wam część żywej debaty w dziedzinie, w której nie jestem ekspertem. Chodzi o bogacenie się państw trzeciego świata. Debata zasadza się na naczelnym pytaniu: „Czy kraje rozwinięte mają moralne prawo decydować, w jaki sposób kraje rozwijające się tworzą energię elektryczną?”. Jestem osobą, ogólnie rzecz biorąc, proekologiczną, więc początkowo wyznawałem dość ograniczony pogląd, iż powinno się odwodzić biedniejsze kraje od spalania zasobów naturalnych, które znalazły się pod lub nad ziemią zajmowanego przez nie rejonu świata. Okazuje się jednak, że taka brudna produkcja prądu może spektakularnie przyspieszyć rozwój państw. Efektem etycznym jest w tym wypadku zwiększenie dostępu do edukacji, opieki zdrowotnej czy chociażby lepsze odżywianie. Gdy kraje rozwijające się bogacą się w wyniku spalania zasobów naturalnych, zaczynają w końcu przejawiać tendencję do przechodzenia na czyste źródła energii! Zwolennicy tej tezy twierdzą, że państwa rozwinięte powinny jedynie asystować krajom rozwijającym się i udostępniać im wyniki badań i technologie pozwalające na budowę odnawialnych źródeł energii. To wszystko jest dla mnie tym ciekawsze, że nawet w tej dyskusji mogłem odnaleźć elementy filozofii

bitcoina, który z nieokiełznanego prądożercy przeistoczył się w ekologa, i którego używamy przecież – między innymi – do walki z ubóstwem.

Czy da się odejść od bitcoina?

Uff… Myślę, że przytoczyłem tu wystarczającą liczbę przykładów, żeby zasiać niepewność w kontekście utartych sloganów i zachęcić do krytycznego spojrzenia na wszelkie doniesienia o nieekologiczności kryptowalut. Musimy wymagać od naukowców naprawdę przekrojowych analiz wpływu kryptowalut na środowisko naturalne, które uwzględniają wiele czynników, zanim sformułują oni ostateczne i niepodważalne werdykty.

Skalę napięć dotyczącą opinii na ten temat niech zobrazuje przykład z flarami gazowymi (a więc dobrze, że go przytoczyłem!). Pomysł stosowania flar gazowych do zasilania kopalni bitcoina jest dyskredytowany przez część środowiska kryptowalutowego, która utrzymuje, że flary powinny być zlikwidowane wraz ze zlikwidowaniem wydobycia ropy. Bitcoin zaś – według tych ludzi – koniec końców nie jest ekologiczny i powinien być zakazany.

Ten podział środowiska kryptowalutowego jest efektem powstania nowej generacji kryptowalut, które zamiast prądożernych algorytmów Dowodu Pracy (*Proof of Work*) stosują wspomniane wcześniej algorytmy Dowodu Udziału (*Proof of Stake*). Dowód Udziału nie wymaga ponadnormatywnego zużycia energii, zachowując jednocześnie większość zalet kryptowalut. I o tę „większość” chodzi przeciwnikom Dowodu Udziału. Większość to prawie wszystko, a „prawie” – jak wiadomo – robi wielką różnicę.

Przeciwnicy Dowodu Udziału nie są gotowi na taki kompromis i nie uważają alternatywnych systemów kryptowalutowych za niezależne na tyle, by móc powierzyć im pokoleniowy majątek. I mają dużo racji. Dlaczego?

Najpierw postarajmy się zrozumieć, jak działa Dowód Udziału i czym się różni od Dowodu Pracy. W kryptowalutach opartych na Dowodzie Pracy mamy górników – teoretycznie każdy może być górnikiem! – którzy kopiąc (wydobywając) kryptowalutę, zużywają energię. Przypomnę, że owo „kopanie" polega na złożonych obliczeniach, dzięki którym górnicy zatwierdzają transakcje. Górnicy są więc walidatorami. Jeśli uda się im znaleźć pożądaną przez kryptowalutę sumę kontrolną zatwierdzanego bloku w blockchainie, dostają nagrodę w postaci stosownej liczby monet – czyli jest tak, jakby je wykopali. Bogacą się, kopiąc.

Tymczasem waluty oparte na Dowodzie Udziału zabezpieczają swoją niezależność, wiarygodność i nienaruszalność zastawem, udziałem, kaucją – jak zwał, tak zwał. Tam też są walidatorzy i też zatwierdzają transakcje, ale przede wszystkim ci walidatorzy to nie górnicy, i nie każdy może być walidatorem. Żeby nim być, trzeba mieć (znaczący) udział w danej kryptowalucie. Liczba walidatorów w zależności od waluty waha się od kilkuset do kilku tysięcy – jest ich nieporównywalnie mniej niż górników w Bitcoinie, stąd oszczędności w zużyciu energii. Istnieje reguła, że jeśli walidator nie przestrzega zasad gry – czyli zasad zatwierdzania transakcji i weryfikowania uczciwości w sieci – traci swój udział. Czy widmo utraty udziału jest zatem wystarczającym batem do zabezpieczenia kryptowaluty przed potencjalnymi nadużyciami ze strony walidatorów? Odpowiedzi na to pytanie usilnie poszukuje dział nauki zwany teorią gier – niestety, różnorodność systemów i ich krótka, bo zaledwie kilkuletnia historia bardzo to utrudnia. Póki co, nie ma odpowiedzi jednoznacznej. Daje to pożywkę spolaryzowanej dyskusji, przypominającej nasze rodzime

spory polityczne.

Dlaczego jakiś walidator chciałby oszukać system i stracić swój udział? Można sobie dość łatwo wyobrazić taką sytuację: jakiś podmiot wchodzi w posiadanie znaczących udziałów w blockchainie konkurencyjnym do swojego i sabotuje jego pracę. Traci udział, ale taki jest wkalkulowany koszt jego kreciej roboty. Prezesi też muszą mieć udziały w firmach, którym przewodzą (to tak naprawdę bardzo dobra analogia z walidatorami), a przecież też czasem zdarza się, że z jakichś powodów umyślnie działają na ich niekorzyść.

Ja uważam, że mamy miejsce dla obu systemów, choć możliwe, że rynek walut Dowodu Pracy skurczy się tak, że pozostanie na nim wyłącznie bitcoin. Krajobraz świata kryptowalut dopiero się wyłania i nie do końca możemy pozwolić sobie na bazowanie wyłącznie na ekologicznym udziale, kaucji, zastawie. Jednocześnie nie będzie już prawdopodobnie nowych systemów *Proof of Work*, a nawet gdyby się pojawiły, na pewno zaczną swój żywot jako systemy *Proof of Stake*. *Proof of Work* to głęboka woda, na którą nikt od razu nie będzie się rzucał – duży nakład pracy górników, aby zapewnić bezpieczeństwo i nienaruszalność systemu, to coś, co buduje się z czasem. Jeżeli chodzi o istniejące systemy, obserwujemy masową migrację: Dowód Pracy ustępuje powoli Dowodowi Udziału.

Jeśli mam się dalej pobawić w wieszczenie, to uważam również, że znaczenie bitcoina bardziej się… hm… znormalizuje. Z wiarygodnej przechowalni majątku zacznie ewoluować do pomostu łączącego świat stuprocentowo wirtualny z namacalnym i rzeczywistym.

Wróćmy do ekologii. Obecnie bitcoin wykorzystuje niecały procent światowej produkcji energii elektrycznej. Jego najwierniejsi zwolennicy zwani maksymalistami utrzymują, że w przypadku migrowania światowych

finansów do zdecentralizowanej domeny kryptowalut zużycie prądu przez bitcoinowy blockchain może sięgnąć pięciu procent.

A o tym, że z bitcoinem jeszcze długo się nie rozstaniemy, przekonuje mnie chociażby wejście do gry tak renomowanych firm jak Intel. Intel stworzył specjalizowany układ do koparek kryptowalutowych (Intel Blockscale ASIC), co ma wspomóc tworzenie niezawodnych i oszczędnych urządzeń.

Wnioski końcowe

Podsumuję ten rozdział tak: ostateczne wnioski i werdykty na temat ekologii kryptowalut można wysnuć dopiero po uwzględnieniu wszystkich związanych z nimi czynników. Dziś jest na pewno zbyt wcześnie na jednoznaczny osąd. Podsumowanie wpływu bitcoina na środowisko jednym procentem światowej konsumpcji prądu nie mówi absolutnie nic o emisji gazów cieplarnianych. Sama emisja gazów natomiast – nawet dobrze oszacowana – pomija całe spektrum potencjalnej degradacji środowiska zanieczyszczeniami, hałasem i dewastacją krajobrazu. Kryptowaluty spalają prąd, jedne więcej, inne miej. Ale – jak pokazałem w przykładach – potrafią też być bardzo ekologiczne. Szczególnie zważywszy na korzyści, jakie nam dają.

8

Dowód Istnienia

– Janku, po co robisz zdjęcia samochodu? Gdy będziemy wyjeżdżać z parkingu, kamera przy szlabanie zrobi nam fotkę i prześle ją do wypożyczalni.

– A ja wolę ją zrobić samemu. I przesłać do blockchaina. Dzięki temu mam dowód, że o tej konkretnej godzinie w tym konkretnym miejscu ten oto samochód miał już tę rysę. Patrz, całkiem spora… Nie chcę za nią odpowiadać.

– O, rzeczywiście rysa, i to z wgnieceniem… I myślisz, że oni uznają to w razie sporu?

– No jasne! Blockchain to nienaruszalna i w pełni audytowalna baza danych! Jeśli wypożyczalnia będzie się upierać, że to ja zrobiłem tę rysę, to prześlę im stosowne zdjęcie. Załączę link do eksploratora blockchaina i wszystko będą mogli sobie sprawdzić: podpis w blockchainie będzie się zgadzał z podpisem zdjęcia, które wyślę, czas podpisu wskaże, że rysa na samochodzie już była przy wypożyczeniu, a my oddaliśmy go w takim stanie, w jakim go wypożyczyliśmy.

Istnienie i czas

Kryptowaluty to zupełnie nowa klasa systemów. I to obiektywnie rzecz biorąc. Dysponują przełomowymi rozwiązaniami i zapewniają narzędzia, dzięki którym z tych rozwiązań można korzystać.

Przypominasz sobie, jaką rewolucją okazał się arkusz kalkulacyjny? Niby tylko przeniósł do pamięci komputera tabele wypełnione liczbami i umożliwił ich sumowanie, kopiowanie i wykonywanie różnych innych operacji na danych (i to na wielu wierszach i kolumnach), a wkrótce stał się programem wykorzystywanym nie tylko przez księgowych. W kolejnych wersjach obrastał w coraz więcej funkcjonalności: pojawiły się wykresy, statystyczna analiza danych i tak dalej. Dziś trudno sobie wyobrazić życie bez arkusza kalkulacyjnego (choć oczywiście sporo osób nienawidzi Excela).

Wspominam tu o arkuszach kalkulacyjnych, żeby jako analogię do ich narzędzi i funkcji omówić jedno z podstawowych narzędzi blockchaina: jest nim Dowód Istnienia (*Proof of Existenc*e, PoE). I gwarantuję ci, że ta prosta z pozoru funkcjonalność jest też… rewolucyjna.

Dowód Istnienia jest informacją zapisaną w blockchainie. Jest transakcją. Każda transakcja ma pole „wiadomość” (można o nim myśleć jak o tytule przelewu). W takim polu możemy zamieścić dowolną informację. Czy pamiętacie jeszcze funkcję hashującą? Tę, przy pomocy której górnicy bitcoina próbują zatwierdzać bloki dołączane do łańcucha? Ta funkcja jest bardzo uniwersalna i może służyć także do innych celów. Może zamienić, dajmy na to, zdjęcie w ciąg znaków nazwany hashem. Ten ciąg znaków, zbitka cyfr i liter, jest identyczny dla konkretnego zdjęcia, niezależnie od komputera, kraju czy języka systemu, który go oblicza, korzystając z funkcji hashującej. W poprzednich rozdziałach porównywałem funkcję hashującą do miksera, który miksuje owoce i przygotowuje koktajl. Tutaj do naszego miksera wkładamy zdjęcie i już w zmiksowanej postaci publikujemy je w blockchainie, czyli w publicznej, ogólnodostępnej bazie danych. Taki ciąg znaków może być miliony razy mniejszy niż zdjęcie. A ponieważ hashowanie to proces nieodwracalny

(podobnie jak miksowanie) nie da się odtworzyć zdjęcia na podstawie hasha, czyli – przypominam – charakterystycznego ciągu znaków wygenerowanego dla zdjęcia przez funkcję hashującą.

Co dalej z tym całym hashem zdjęcia?

Wróćmy do przykładu z wypożyczalnią. Jan oddaje samochód. Podczas oględzin przedstawiciel wypożyczalni zauważa na drzwiach samochodu brzydką rysę z wgnieceniem. To uszkodzenie mogło faktycznie powstać na parkingu już po oddaniu samochodu przez poprzedniego kierowcę. Przed tym, jak samochód przejął Jan, ktoś parkujący obok mógł nieostrożnie wyjechać ze swojego miejsca. Za uszkodzenie nie odpowiada ani poprzedni kierowca, ani Jan, ale to Jana wypożyczalnia chce obciążyć odpowiedzialnością za powstałą szkodę.

Dobrze, że Jan udokumentował uszkodzenie. wykonując zdjęcie smartfonem. Takie źródło nie jest jednak obiektywne. Bardzo prosto zmanipulować dane zdjęcia, na przykład datę jego powstania. I tu wkracza supermoc kryptowalut! Poprzez opublikowanie hashu zdjęcia w blockchainie przed wyjazdem z parkingu Jan „zakotwiczył” je w czasie w absolutnie niekwestionowany sposób. Dzięki takiej transakcji może teraz wysłać zdjęcie do wypożyczalni i tym samym wykazać, że samochód miał paskudną rysę już wcześniej. Jan, wysyłając je, dołącza link do transakcji w blockchainie, w której znajduje się hash fotki z rysą – rysą powstałą jeszcze przed przejęciem samochodu.

W wypożyczalni patrzą na zdjęcie. Owszem, widać na nim rysę, data i czas też się zgadzają, ale przecież nie można ufać każdemu klientowi. Zdjęcie trafia więc do oprogramowania wypożyczalni, które za pomocą funkcji hashującej niezależnie oblicza hash fotki i porównuje go z tym, który jest publicznie dostępny w blockchainie. Hashe zgadzają się. Zdjęcie jest autentyczne i faktycznie przedstawia stan samochodu sprzed

użytkowania go przez Jana, który tym samym uwolnił się od niesłusznych oskarżeń.

Połączenie Dowodu Istnienia z czasem nazywamy Dowodem Czasu, czyli *Proof of Time*. Dzięki blockchainowi w wielu sytuacjach robienie zdjęcia, hashowanie go i zapisanie hasha w blockchainie może bardzo się przydać – dzięki temu możemy udowodnić, że zdjęcie powstało o konkretnym czasie lub wcześniej, ale nigdy później!

Powyższy przykład można by odwrócić, bo nieuzasadnione roszczenia zdarzają się też w stronę firm. Linie lotnicze mogłyby fotografować powierzane im bagaże przy check-inie, żeby dokumentować ich stan. Jeśli na zdjęciu przyjmowany bagaż wygląda na nieuszkodzony (lub uszkodzony), jest dokładnie taki w chwili check-inu lub wcześniej, ale nigdy nie później. Można by zatem łatwo oddalać reklamacje podróżnych, którzy przychodzą na lot z uszkodzonym bagażem.

Kolejną przełomową możliwością, jaką oferują kryptowaluty, jest zapisanie w publicznej bazie danych – blockchainie – naszych pomysłów, utworów i wszelkiego rodzaju dzieł. Dzięki temu, że będą reprezentowane wyłącznie przez hash, nikt nie pozna ich treści. Jednak gdy powstanie spór wokół praw autorskich – na przykład nasz pomysł zostanie skradziony przez nieuczciwą konkurencję – będziemy mogli, podobnie jak w przypadku hashowanych zdjęć, udowodnić, że dokument opisujący dany pomysł powstał dokładnie w określonym czasie w przeszłości i że my jesteśmy jego autorami. Jest to Dowód Autorstwa, *Proof of Authorship*.

Opisałem tu niepodważalne połączenie świata wirtualnego ze światem rzeczywistym, co przed erą blockchaina było bardzo trudne do zrealizowania. Blockchain sprawdzi się też w wielu sytuacjach z codziennego życia, a poprzez powiązanie ze sobą tożsamości i innych rozmaitych danych uprości mnóstwo procesów.

Sztandarowym przykładem są wszystkie te sytuacje, w których musimy przedstawić numer licencji, aby otrzymać jakiś produkt, na przykład oprogramowanie opłacone przez naszego pracodawcę. Posługując się wirtualną tożsamością w sklepie internetowym lub u dystrybutora oprogramowania, legalizujemy to oprogramowanie, podając Dowód Istnienia licencji przypisanej do tej tożsamości. Jest to rozwiązane o wiele pewniejsze i bezpieczniejsze dla wszystkich.

Czymś bardzo podobnym do Dowodu Istnienia jest Dowód Nieistnienia. Za jego pośrednictwem udowadniamy brak kar, punktów karnych, zaległych opłat czy negatywnych opinii. Dowód Nieistnienia spowodowanych wypadków to droga do zniżek przy wykupie ubezpieczenia.

Owad w bursztynie – raz jeszcze

Czy dostrzegasz powtarzający się w tych przykładach stały element? Tak, chodzi o absolutną nienaruszalność zapisanych danych. Przez to, że mamy gwarancję ich niezmienności – przypominasz sobie owada zatopionego w bursztynie? – możemy budować nowe funkcjonalności. I to właśnie jest najważniejsze w kryptowalutach. Nie monety, nie szczegóły techniczne, lecz nienaruszalność wirtualnych publicznych danych.

Żeby wszystkie te dowody mogły się przydać, potrzebny jest rzecz jasna blockchain. Może być to jeden z publicznych kryptowalutowych blockchainów, może być to blockchain dedykowany, na przykład blockchain inteligentnego miasta. Nieodzowna będzie aplikacja na smartfonie, która obsłuży wszystkie złożone akcje użytkownika, takie jak chociażby zamiana zdjęcia lub innego dokumentu w hash. Dobrze by było,

żeby ta aplikacja zawierała moduł obsługujący naszą tożsamość lub współpracowała z inną aplikacją, która ją potwierdza. Dla każdej akcji możemy wygenerować nowy adres, aby nasze ślady w publicznej bazie danych nie były połączone. Wówczas drugiej stronie transakcji naszym kryptograficznym podpisem udowodnimy, że za wszystkimi akcjami kryje się jedna i ta sama tożsamość.

Na początku tego rozdziału napisałem, jak niezwykle przełomowy w wielu dziedzinach okazał się arkusz kalkulacyjny – prosta koncepcja tabeli wypełnionej cyframi, przeniesiona z papieru do pamięci komputerowej. I choć kryptowaluty i blockchain to o wiele wyższa szkoła jazdy, otwierają zupełnie nowe możliwości dzięki jednej, wydawałoby się oczywistej idei: idei nienaruszalności danych w publicznej, ogólnodostępnej bazie, której bezpieczeństwo wynika z samego jej charakteru działania. Owad zatopiony w narastającym wokół niego bursztynie. Transakcja zamknięta w osłonie z kolejnych, i jeszcze kolejnych, i jeszcze kolejnych transakcji.

Zanim blockchain się upowszechni…

Przykład z wypożyczeniem samochodu nie jest przecież oderwany od rzeczywistości. Bywa, że załatwienie sprawy z lotniskową wypożyczalnią to droga przez mękę. Zdjęcie w aplikacji weryfikującej czas i miejsce wywoła przynajmniej chwilę refleksji konsultanta, zanim nas zbędzie i przełączy do kolejnej infolinii. Nawet jeśli nie macie możliwości shashowania zdjęcia i skorzystania z blockchaina, na wszelki wypadek róbcie zdjęcia wypożyczonym samochodom.

9

Notariusz

– Będziesz dziś po południu?

– Nie dam rady, mam umówionego notariusza, zakładam z Krzyśkiem spółkę…

– O, gratulacje! Ale myślałam, że teraz to tylko kilka kliknięć i gotowe.

– Niestety. To dość złożona umowa, zapowiada się długie czytanie… A nawet gdyby była prosta i krótka, i tak trzeba ją podpisać u notariusza.

Notariusz kontra blockchain

Po co nam notariusze i akty notarialne? O tym, że to konieczność, mówi wprost nasze prawo. Istotne sprawy dotyczące naszego życia, by zyskać moc prawną, muszą zostać potwierdzone aktem notarialnym. Między innymi tak właśnie państwa rozciągają opiekę nad działaniami obywateli.

Piszę to zupełnie bez ironii, która często pojawia się, gdy opisujemy biurokratyczne ramię struktur państwowych. Przecież w interesie nas wszystkich jest to, by wszelkie umowy były przestrzegane, a prawa własności – dochowywane. To gwarancja rozwoju, dobrobytu i dobrostanu.

Co należy do zadań notariusza? W każdym kraju ma nieco inny zakres obowiązków. Skupmy się najpierw na notariuszu pracującym w Stanach

Zjednoczonych. Główną i często jedyną jego rolą jest sprawdzanie autentyczności dokumentów będących przedmiotem umów. Przykładowo: sprzedaż ziemi wymaga aktu własności. Dzięki notariuszowi strona kupująca może być pewna, że przedstawiony przez sprzedającego akt własności jest autentyczny. Drugim zadaniem jest poświadczanie zawarcia umów. Notariusz może nie znać treści umowy, ale jest niepodważalnym świadkiem jej podpisania. To bardzo ważna kwestia: takie poświadczenie minimalizuje ryzyko oszustw i nieuczciwości we wszelkich przedsięwzięciach.

Czy nie przypomina ci to czegoś? Sprawdzenie autentyczności, poświadczenie zawarcia umowy? Przecież to wszystko dokonuje się w blockchainie! Sęk w tym, że blockchain w powszechnej świadomości jest nieodłącznie związany – a wręcz utożsamiany – z kryptowalutami. Jest więc poniekąd na straconej pozycji, która skutecznie utrudnia mu wyrwanie się ze świata finansów. Pieniądze. Waluty. Kryptowaluty. Blockchain. Tymczasem blockchain to nie tylko narzędzie do zatwierdzania transakcji. To szeroko pojęta platforma zaufania. I to jest rdzeń jego istnienia.

Zdarzało mi się wcześniej używać słowa „księgowość” w odniesieniu do blockchaina – wszak blockchain to idealny księgowy, który prowadzi rejestr naszych transakcji, naszą księgę przychodów i rozchodów. Przede wszystkim jednak blockchain jest świadkiem naszych działań, i to takim, którego poświadczenie jest niepodważalne. Jest zupełnie jak notariusz. Bardzo często zresztą mówi się o blockchainie jako wirtualnym notariuszu.

Czy zatem blockchain może zastąpić notariusza? Nie, przynajmniej jeszcze nie teraz. Co prawda akty własności i księgi wieczyste w wielu krajach świata są zdigitalizowane, ale stanowią wyłącznie elektroniczne archiwum zapisów sądowych. To notariusz dysponuje kopią przeniesienia aktu własności i to on wysyła do sądu dokumenty, na podstawie których sąd

aktualizuje daną księgę wieczystą. Żyjemy w XXI wieku, a wszystko nadal sprowadza się do zwykłej kartki, kawałka papieru. Owszem, ta zwykła kartka to też technologia, tyle że… już dość stara. Wciąż jednak to właśnie ona – kartka – ma moc dokonywania zmian stanu prawnego obywateli, nadaną jej przez aparat państwowy.

Jak to zmienić? Jednym ze sposobów jest wyposażenie obywateli w najpotężniejszą broń chroniącą poufność: kryptografię. Możemy wyobrazić sobie system, który – podobnie jak elektroniczne księgi wieczyste – przechowuje rejestr właścicieli i ich własności. Poszczególne zapisy tego rejestru chronione są kluczami prywatnymi. Przypomnij sobie naszą podróż przez świat elektronicznego pieniądza, w szczególności transfery środków pieniężnych. Tylko właściciel klucza prywatnego do portfela może zlecić transfer przechowywanych w nim pieniędzy. I analogicznie – wyłącznie właściciel nieruchomości może za pomocą swojego klucza prywatnego dokonać transferu własności, przekazując ją innemu podmiotowi. Jeśli żadna ze stron nie posiada klucza prywatnego do adresu z zapisem jakiegokolwiek prawa własności, transfer tejże własności po prostu się nie odbędzie. Trzeba pamiętać o tym, że to rozwiązanie jest trochę jak miecz obosieczny: pełne samostanowienie to także zgoda na wzięcie na siebie pełnej odpowiedzialności…

Dysponując kluczem prywatnym mielibyśmy całkowitą swobodę wykonywania działań prawnych, które dziś wymagają notarialnego potwierdzenia (przenoszenie własności, upoważnianie i tym podobne).

Wróćmy jednak do kwestii notariusza – a właściwie notariusza w rozumieniu anglosaskim, bo to właśnie anglosaska odmiana notariatu jest praktycznie tożsama z tym, jak działa blockchain. Skoro kryptografia znakomicie zastępuje niepodważalnego świadka, a blockchain zapisuje

nasze działanie i przechowuje je na wieczność, czy można wysłać wszystkich notariuszy na emeryturę?

Na pewno nie w Polsce. W Polsce notariusz to nie tylko świadek, ale także doradca w kwestiach prawnych. Zna treść aktu prawnego, bo odczytuje go stronom, i dba o jego zgodność prawną. Jest więc swego rodzaju doradcą prawnym – to funkcja, która odróżnia go od jego kolegi z USA i od blockchaina.

Ciekawym przykładem – idealnym na koniec tej sekcji – jest system rejestru nieruchomości w Gruzji, który niejako wyprzedza tradycyjną notarialną epokę, korzystając z najnowocześniejszych rozwiązań. I to z wielkim powodzeniem, co wynika z raportu OECD porównującego rozwijające się gospodarki, takie jak Ghana czy Gruzja. W Ghanie 80% nieruchomości cierpi z powodu wybrakowanej dokumentacji, za to Gruzja jest czwartym krajem na świecie pod względem prostoty obsługi rejestracji nieruchomości. Gruzja stosuje smartkontrakty, co w dodatku – jak przystało na każde nowoczesne zastosowanie blockchaina – odbywa się na ekologicznej platformie niewymagającej prądożernego kopania.

Bezpieczeństwo

Nie sposób nie zapytać o potencjalne problemy. Co się stanie, jeśli zgubimy klucz? A jeśli zostanie on nam skradziony bądź wyłudzony? Kwestie te rozwiązuje – przynajmniej w dużej części – sama kryptografia. Klucze kryptograficzne to ciekawe narzędzia. Możemy na przykład tak skonfigurować podpis wymagający klucza, by żądał on… wielu kluczy. Trzech z pięciu, dajmy na to, we wtorek, i czterech z pięciu w sobotę. Nie ma tu żadnych ograniczeń. Tym sposobem możemy opiekę nad stanem

prawnym nieruchomości rozdzielić na kilka osób. Nasuwa się od razu pomysł wykorzystania tej metody do ułatwienia kredytowania nieruchomości. Obecnie, kiedy do chwili spłaty kredytu bank jest właścicielem nieruchomości, trzeba borykać się z wieloma formalnościami. Można zatem wybrać jeden klucz, który nadaje uprawnienia do transferu własności, i kilka innych kluczy, które legitymizują użytkowanie nieruchomości. Życie najemców też można by w ten sposób ułatwić: ich klucz prywatny uprawniałby ich do obsługi spraw związanych z najmem i pozwalał na przykład zarejestrować się w przedsiębiorstwie wodociągowym czy u dostawcy energii.

Taki klucz prywatny, strzegący naszego majątku lub naszych praw, musi być kluczem sprzętowym – małym urządzeniem chroniącym cyfrową zawartość klucza. Gdy zgubimy urządzenie, możemy je odtworzyć. Możemy posiadać kilka jego kopii. Gdy ktoś je znajdzie, nic z nimi nie zrobi. Możemy również taki klucz rozdzielić na kilka części, które pozwolą go odtworzyć wyłącznie wtedy, gdy znajdą się razem w jednym miejscu.

Rozwiązania ułatwiające korzystanie z tych kluczy prywatnych strzegących naszej własności (i sekretów!) już są obecne na rynku, co więcej – są one kompletne. Niestety, są też często ignorowane. Wydaje mi się, że dopiero dotarcie do zbiorowej świadomości z przystępnym objaśnieniem wszelkich możliwych sposobów zabezpieczenia swoich kluczy odblokuje szerokie zastosowanie blockchaina w obsłudze naszych codziennych spraw.

Smartkontrakty – nowy etap (r)ewolucji

Kolejnym uproszczeniem naszego „życia prawnego” byłoby przeniesienie do blockchaina wszelkich możliwych aktów, które może spisać notariusz. Spadek, zmiana własności nieruchomości, zawarcie umowy spółki, udzielenie upoważnienia. Wszystko to może być katalogiem programów, które w świecie blockchaina w zasadzie już działają i nazywają się smartkontraktami. Smartkontrakt żyje w blockchainie i opisuje zasady, reguły, ustalenia, na jakie godzą się obie zawierające go strony – czyli funkcjonuje zupełnie jak umowa.

Smartkontrakty to nowinka drugiej generacji blockchainów, których prekursorem było ethereum. A oto powód do radości: hipotetyczny państwowy blockchain, który mógłby pełnić funkcję strażnika i legislatora naszych działań prawnych, byłby całkowicie ekologiczny! Ale że państwowy? Gdzie tu decentralizacja? Otóż państwowość blockchaina w tym konkretnym przypadku ma dużo sensu. W interesie zawierających umowy i tworzących akty prawne jest to, by węzły zatwierdzające zmiany w takim blockchainie reprezentowały państwo. Tożsamość w takiej państwowej blockchainowej platformie byłaby przydzielana automatycznie każdemu nowo narodzonemu obywatelowi.

Przyjrzyjmy się nieco bliżej działaniu smartkontraktów na przykładzie smartkontraktu spółki z ograniczoną odpowiedzialnością. Nie dość, że jest to najpopularniejszy wśród stosowanych smartkontraktów, to jest do tego bardzo intuicyjny. Opisuje przynależność udziałów, które są w nim zapisane, do poszczególnych udziałowców reprezentowanych przez klucze prywatne. Taki smartkontrakt może być również właścicielem środków spółki i dokonywać zmian ich stanu wyłącznie wówczas, gdy zbierze się stosowne kworum udziałowców. Bardzo podobnie co do zasady obsługiwane byłyby spółki akcyjne czy komandytowe. Publiczny, sprawdzony, nawet określony ustawą katalog smartkontraktów mógłby

oferować obywatelom wszelkie dostępne w prawie aspekty aktywności, które wymagają notarialnego poświadczenia – i to zarówno jeśli chodzi o działalność gospodarczą, jak i dotyczące spraw osobistych.

Twoja własna waluta? Skorzystaj z ERC-20!

Ciekawostka: w blockchainie ethereum bardzo ogólną postacią smartkontraktu dla spółki z ograniczoną odpowiedzialnością lub spółki akcyjnej jest program o nazwie ERC-20 (skrót od *Ethereum Request for Comments 20*). Służy on do ustanowienia swojej własnej waluty. Tak, jednym kliknięciem możemy stworzyć nową walutę! Monetami – tokenami – takiej waluty są udziały w smartkontrakcie, czyli udziały spółki lub jej akcje. Można w tym dostrzec spore podobieństwo do tradycyjnej waluty, którą zabezpiecza i której nadaje wartość bank centralny – tu mamy udziały, które zabezpiecza i którym nadaje wartość majątek spółki, czyli… nasz smartkontrakt. Oczywiście w chwili ustanowienia ta nowa waluta jest zwykle bezwartościowa – w końcu są nią udziały nowej spółki, która jeszcze nie dała się poznać na rynku. Jeśli jednak spółka zaczyna tworzyć coś ciekawego – oferować pożądane usługi lub produkty – jej wartość rośnie, a wraz z nią wartość kryptowaluty.

Najlepiej to zrozumieć na przykładzie (choć pewnie przypominasz sobie rozdział o wypożyczalni, w którym dyskutowaliśmy nadawanie wartości nowej kryptowalucie – tu będzie podobnie).

Aby monety ERC-20 nabrały wartości, muszą zapewnić pożądaną funkcjonalność. Musi być coś, co da się za nie kupić – na przykład obejrzenie filmu w serwisie streamingowym. Możemy sobie wyobrazić taki serwis, który udostępnia filmy, ale nie w ramach miesięcznej subskrypcji,

jak Netflix i inni, lecz w zamian za monety wysłane do jego portfela z poziomu przeglądarki internetowej. Nasza przeglądarka będzie zatem zachowywać się jak portfel kryptowalutowy. Na giełdzie zasilimy go „filmomonetami” i będziemy mogli korzystać z oferty serwisu. Zauważcie, że dzięki sprzedaży monet ERC-20 na giełdzie, autorzy monet zyskują środki! Waluta już nie jest „pusta”, bez pokrycia, jej wartość zaczyna podlegać prawom rynku. Oczywiście ze środków ze sprzedaży monet nasi walutowi przedsiębiorcy muszą zbudować i utrzymać serwis filmowy.

Dostrzegasz już zalety takiego rozwiązania? Serwis streamingowy – to jeden z wielu przykładów – nie będzie znał naszej tożsamości, lecz jedynie anonimowy adres, który stworzymy specjalnie do korzystania z serwisu. Nasze zwyczaje i upodobania będą ukryte przed reklamodawcami, a dane naszych kart kredytowych już nigdy nie wyciekną – bo ich tam po prostu nie będzie.

To jeszcze nie koniec zalet. Z czasem może się zmienić sama funkcjonalność monet. Tokeny są przecież tak tanie w obsłudze, że możemy płacić nimi nie za cały film, ale za poszczególne sceny, fragmenty czy nawet… klatki! Jeżeli film będzie słaby, szybko zrezygnujemy z jego oglądania – bez konieczności płacenia za całość. Podobnie jeśli bardzo nam zależy na obejrzeniu tylko jednej, ulubionej sceny – zapłacimy tylko za nią.

Tak wygląda to wszystko od strony klienta. A od strony spółki? Mechanizm smartkontraktu sprytnie połączył utworzenie waluty i start-upowej spółki, pozwalając twórcom serwisu streamingowego zdobyć środki na jego prowadzenie. Chcąc przenieść go do realiów świata rzeczywistego, natkniemy się na mnóstwo formalności do załatwienia. A załatwianie formalności to wielki hamulec innowacji. Hamulec, którego się pozbywamy, korzystając z usług naszego blockchainowego notariusza.

Inne przykłady, kiedy blockchain zastępuje notariusza i lepiej się sprawdza? Smartkontrakt rodzinnej fundacji. Strzegący pokoleniowego majątku i jednocześnie zabezpieczający dostęp do niej starszeństwem kluczy lub stosownym kworum. Tego typu sytuacje można mnożyć. Możliwości są nieograniczone.

Umowy i podpisy

Podpisanie dowolnej umowy nie wymaga jednak stosowania smartkontraktu. Jest to podstawowa funkcjonalność blockchaina i nowoczesnej kryptografii, która już nam pomogła przy wypożyczaniu samochodu. Tak jak zdjęcie zwirtualizowane w blockchainie, tak i każda umowa może pozostać tajna, ale jej sygnatariusze mają dowód jej podpisania, ze wszystkimi niepodważalnymi danymi takimi jak czas złożenia podpisów. Tym sposobem cała tradycyjna działalność notarialna, opierająca się na tworzeniu wypisów, odpisów i potwierdzeń, traci rację bytu. Te dane są osiągalne zdalnie, w publicznej, nienaruszalnej, pseudoanonimowej bazie danych. Tylko ich właściciele wiedzą, jak je odnaleźć celem przedstawienia ich w razie potrzeby zainteresowanym stronom.

Warto wspomnieć, że przez ostatnie lata, kiedy świat borykał się z pandemią, scentralizowane serwisy cyfrowego podpisywania dokumentów (Adobe Sign, DocuSign i inne) zyskały wielu użytkowników. Niestety, mimo że również bazują na podpisach kryptograficznych, czyli samo podpisywanie jest bezpieczne i weryfikowane, nie chronią stuprocentowo prywatności treści zawieranych porozumień. Umowy niestety trzeba wysłać w postaci cyfrowej do bazy serwisu, gdzie jest

podpisywana z użyciem klucza kryptograficznego. Klucz ten znajduje się pod całkowitą kontrolą serwisu: jego pracowników i wszystkich z dostępem do infrastruktury. Dzięki podpisom cyfrowym zyskaliśmy wygodę podpisywania umów, o jakiej zawsze marzyliśmy (zerwanie z drukowaniem, przesyłaniem dokumentów pocztą bądź kurierem, oczekiwanie na kontrpodpis, gubienie wydruków), ale obniżyliśmy nieco poziom bezpieczeństwa: kartka i długopis zapewniały wyższy.

Weksle i czeki. To nic innego jak transfery środków dokonywane pod szczególnymi warunkami. Również i w tym wypadku smartkontrakt jest najlepszym sposobem cyfrowego zapisu uzgodnionych warunków. Może uwzględniać daty lub inne zależności, na podstawie których zachodzi możliwość zrealizowania transferu pieniężnego. Dodatkowo w swoim kodzie, jeśli taka jest obopólna wola, smartkontrakty czekowe i wekslowe mogą zawierać szczegóły warunków samozniszczenia.

Dobrym przykładem z życia codziennego jest zabezpieczenie umów leasingu wekslem chroniącym interesy leasingodawcy. Słuszne, bo taki weksel istotnie redukuje ryzyko… Co by było, gdyby nieuczciwy leasingobiorca przestał spłacać dzierżawę samochodu i wyjechał nim na długie, bardzo długie wakacje…? Rozwiązaniem jest połączenie kodu weksla z zapisem o własności samochodu. Jeśli dzierżawa samochodu dobiegnie końca lub samochód zostanie wykupiony przez dzierżawcę, to weksel sam ulegnie zniszczeniu. Jeśli jednak na wirtualny adres samochodu nie spłyną środki za jego dzierżawę, wówczas weksel uruchomi się…

„Drżyjcie, notariusze”? Niekoniecznie…

To najbardziej konkretne przykłady, jakie przychodzą mi do głowy, gdy zastanawiam się, jak uznanie blockchaina za platformę zaufania usprawni funkcjonowanie państwa. I nie chodzi mi wcale o ograniczenie instytucji notariusza – bardziej o wyposażenie go, a także obywateli, w narzędzia nowej generacji. Jest to pierwszy taki wynalazek, który z jednej strony charakteryzuje się niepodważalnością umowy dokładnie taką, jak umowa spisana na papierze, a zarazem jest znacznie bardziej odporny na pogodę, złodziei i turbulencje historii.

Wiesz, który z budynków spłonął jako jeden z pierwszych podczas rewolucji październikowej w Petersburgu? Sąd. Spłonął, a wraz z nim akty własności ziem i kamienic ich prawowitych właścicieli. Po to, by tymi kamienicami i ziemiami można było zapłacić kohortom nowych żołnierzy, którzy zmienili bieg historii na co najmniej sto kolejnych lat.

Zapisy w blockchainie nie mogą spłonąć. Nawet jeśli nastąpi blackout, im nic się nie stanie. W tym właśnie tkwi potęga decentralizacji i nienaruszalności.

Faketoshi

W tym rozdziale dużo było o poświadczaniu tożsamości, podpisach cyfrowych, kryptografii i aktach notarialnych. Słowem – o potwierdzaniu i nienaruszalności prawdy zapisanej w blockchainie. To na koniec taka anegdota: w ostatnich latach dość głośnym przypadkiem jest sprawa Craiga S. Wrighta, australijskiego naukowca i przedsiębiorcy, który twierdzi, że to on jest Satoshim Nakamoto, czyli twórcą bitcoina. Niestety, nie zdołał tego wykazać w najprostszy, a zarazem absolutnie niepodważalny sposób. Prawdziwy Satoshi Nakamoto mógłby bez najmniejszego problemu dokonać transferu jednej z najstarszych monet (czyli najwcześniej powstałych), które stworzył w czasie rozwoju oprogramowania. Na podstawie zapisów na forach wiemy, które portfele należą do Nakamoto (u zarania bitcoina była ich ledwie garstka) – w końcu blockchain to publiczna baza danych. Transfer monety z takiego

portfela wyjaśniłby wszystko. Blockchain stałby się w tym przypadku (i w każdym innym!) ostatecznym i prawdomównym świadkiem. Wright nie dokonał takiego transferu. Zapewne dlatego, że nie mógł. Stał się za to uosobieniem wielu nadużyć w świecie blockchaina, a niedawno na Florydzie zakończył się jego proces za oszustwa. W mediach jest teraz określany mianem Faketoshiego.

Język cyfrowych umów

Z uwagi na nieuchronne przeniesienie umów do blockchaina i wyrażenie ich w smartkontraktach (przecież to dosłownie… inteligentne umowy!) badacze i hakerzy tacy jak Henning Diedrich pracują nad językiem przyjaznym jednocześnie dla ludzi i maszyn. Henning wraz z zespołem współpracowników opracował system Lexon specjalnie dla cyfrowych umów, który formułuje je w języku naturalnym, a jednocześnie zapewnia ich jednoznaczną interpretację przez procesor blockchaina. Henning zamierza w ten sposób wesprzeć nadciągającą wielkimi krokami kooperację ludzi i maszyn, z czym wiążą się między innymi następujące dylematy: Jakiego prawa powinny stosować i przestrzegać roboty? Jakiemu prawu musi się podporządkować autopilot w samochodzie? Jednoznaczna interpretacja umów pozwoli także zminimalizować straty (szacowane obecnie na 9% obrotów) wynikające z ich różnego rozumienia przez strony.

10

NFT

Jan zerwał się z łóżka trzy minuty przed spotkaniem zdalnym w pracy. „Zaspałem…”, pomyślał i w tej samej chwili przypomniał sobie, że dziś jego dział ma rozmawiać z bardzo ważnym klientem.

Już trochę mniej nieprzytomnym wzrokiem omiótł swoje mieszkanie. Widok był, delikatnie rzecz ujmując, nieciekawy.

„Koniecznie muszę ustawić jakieś dobre tło”.

Zdjęcie autorstwa Ansela Adamsa – piękny pejzaż, który kupił na niedawnej aukcji NFT – nada się idealnie. Obok, na wirtualnym blacie, który zastępuje kawałek biurka widoczny w kamerze laptopa, Jan stawia wirtualny puchar – wygrał go w zeszły weekend w turnieju szachowym online. Świetna sprawa – jego nowoczesny kształt wspaniale się komponuje z tłem i pokazuje, że Jan ma bogate zainteresowania: fotografia, szachy… Przy okazji puchar jako NFT automatycznie loguje Jana do serwisu szachowego – 10 lat subskrypcji za darmo! Jan uśmiecha się z zadowoleniem, ale zaraz wraca myślami do spotkania. „Co by tu jeszcze…” Ma co prawda bilety NFT na finał ligi, jest zapalonym kibicem, może tak przełamałby lody z klientem… Nie… Co za dużo, to niezdrowo. Ansel Adams. Szachy. Wystarczy. Wyrafinowany klient zwróci uwagę i doceni.

„O, spotkanie się już zaczyna. No nie, Pola łączy się spod tego swojego awatara NFT znudzonej małpy. Szczęściara! Kupiła go już dawno za jakieś trzysta dolców, a nie dalej jak wczoraj ktoś chciał go od niej odkupić za dziesięć tysięcy…

Dobra. Spotkanie. Skupienie”.

– Dzień dobry wszystkim…

Nasza migracja do świata wirtualnego

Czym jest NFT? Chyba każdy aktywnie korzystający z internetu natknął się już na ten skrótowiec. Te trzy litery pojawiają się głównie w popularnych artykułach opisujących wydawanie gigantycznych kwot na obrazki, filmiki i inne unikatowe „cyfrowe dzieła sztuki". W samym 2021 roku na tylko jednej platformie NFT wartość rynku tokenów wzrosła ze 150 milionów do 5 miliardów dolarów!

A skoro skrót NFT dotyczy pieniędzy, to może ma jakiś związek z ETF (*Exchange-Traded Funds*), czyli funduszami inwestycyjnymi?

Nie. NFT to nie fundusz inwestycyjny.

NFT to elektroniczny dowód własności dowolnej rzeczy.

I najprawdopodobniej rynek NFT w postaci, w jakiej znamy go dziś, zbankrutuje.

Mimo to NFT to jedna z najciekawszych technologii tworzących fundamenty wirtualnej rzeczywistości, do której prędzej czy później przeniesiemy większość naszej aktywności.

O nieuchronności migracji do świata wirtualnego mówi się od dawna – trafią tam edukacja, praca, znajomi, rozrywka. Zresztą dzieje się to już teraz, na naszych oczach. Przed pandemią, która z wielu powodów zapisze się trwale na kartach historii naszej cywilizacji, podchodziliśmy do świata wirtualnego bez przekonania, a wręcz ze sporą rezerwą. Nie wierzyliśmy, że to, co robimy „w realu", będzie działać „w wirtualu", i że w ogóle ktoś chciałby tak żyć. Tymczasem okazało się, że… działa! Można zdalnie pracować, uczyć się, spotykać, rozmawiać, urządzać targi, wykładać, brać udział w konferencjach, załatwiać sprawy urzędowe, i to nawet te, które

wymagają poświadczenia tożsamości. Świat wirtualny przestał być wyłączną domeną cyfrowych nomadów – trafiliśmy tam wszyscy i to nierzadko wbrew naszej woli czy chęci – po prostu okazało się, że tylko tak w okresie lockdownu możemy prowadzić w miarę normalne życie. Okazało się także, że rzeczywistość wirtualna daje zupełnie nowe możliwości, wyzwala kreatywność i… koniec końców jest całkiem wygodna!

Jeśli teraz wzbogacimy nasze doznania, zastępując wpatrywanie się w ekran komputera i obiektyw kamerki nową generacją gogli VR (*Virtual Reality*, rzeczywistość wirtualna), które generują obraz do złudzenia przypominający rzeczywistość albo nakładający na ową rzeczywistość nowe, wzbogacające ją elementy AR (*Augmented Reality*, rzeczywistość rozszerzona), zrobi się jeszcze ciekawiej! Czy NFT pomoże nam się urządzić w tej przedwcześnie nastałej przyszłości?

Przekonajmy się!

Dowód własności

NFT jest dowodem własności. Może dotyczyć samochodu, domu, działki, zdjęcia czy obrazu, a także wielu innych dzieł, o czym za chwilę się przekonamy.

Sam pomysł certyfikacji własności unikatowych obiektów – choćby i możliwych do skopiowania lub seryjnie produkowanych – nie jest wcale nowy. Już od czasów wynalezienia kliszy filmowej uznani artyści zarabiali na zdjęciach, wykonując ograniczoną liczbę ich odbitek, czyli kopii. Co w tym przypadku jest oryginałem? Ile jest warta jedna odbitka limitowanej serii? O tym decyduje rynek. Gdy znany fotograf lub grafik komputerowy zadeklaruje, że powstanie tylko dziesięć odbitek zdjęcia lub dziesięć

unikatowych kopii cyfrowego dzieła, wartość takich obiektów rośnie – pod warunkiem, że są chętni na ich zakup. Takie dzieła mają swój unikatowy numer identyfikacyjny i są stuprocentowymi oryginałami, mimo że nie są tradycyjnymi malowanymi obrazami, które powstały w wyniku jedynych w swoim rodzaju pociągnięć pędzlem.

Czas najwyższy na zgłębienie technikaliów i rozwinięcie omawianego skrótu. NFT to *Non-Fungible Token* – niewymienny i niepodzielny token, niewymienna i niepodzielna moneta. Monety lub tokeny kryptowalut – zupełnie jak pieniądz zwykłej waluty – są wymienne i podzielne. Za paczkę cukierków kosztującą cztery złote możemy zapłacić dwoma monetami dwuzłotowymi lub czterema jednozłotowymi – nikomu to nie zrobi różnicy.

Podobnie mają się sprawy w blockchainie ethereum – w niezwykle uniwersalnym blockchainie. Tak uniwersalnym, że jego twórcy nazywają go „komputerem światowym” – dlatego że może obsłużyć dowolną funkcjonalność, podobnie jak zwykły komputer, na którym odpalisz każdy możliwy przeznaczony dla niego program. Wewnętrznie ethereum posługuje się wymiennymi monetami, a posiadacze monet mają własne adresy stanowiące ekwiwalent kont bankowych. Ponieważ jednak własność monet to nie wszystko (podobnie jak w życiu: majątek to nie tylko pieniądze w portfelu i na kontach, ale także rozliczne ruchomości i nieruchomości), potrzebowaliśmy nowego tworu. Potrzebowaliśmy monety, która jest unikatowa pod względem własności. Monety, tokena, w którym zawarta jest informacja: „Jestem własnością Jana”. Potrzebowaliśmy zatem nowej reprezentacji monety.

Pamiętasz, jak tworzy się monety w blockchainie ethereum? Robi się to przy pomocy smartkontraktu. By założyć spółkę akcyjną lub stworzyć własną walutę należy skorzystać ze smartkontraktu ERC-20. (Wiesz, że o smartkontrakcie można myśleć jak o specjalnym programie

wykonywanym przez blockchain kryptowaluty?). By stworzyć unikatową, niewymienną monetę, można użyć standardowych smartkontraktów ERC-721 lub ERC-1155. Można nawet napisać swój własny smartkontrakt – jeśli tylko dysponuje się odpowiednią wiedzą i umiejętnościami.

Tu mała dygresja: oczywiście, że zawsze można napisać swój własny smartkontrakt, ale lepiej stosować standardowe kontrakty, do których nasi klienci – kupcy – będą mieli zaufanie. Zamawiając samochód i mając do wyboru silnik standardowego benzyniaka albo eksperymentalne dzieło domorosłego uczonego, na co byś się zdecydował? Ze względu na niezawodność i bezpieczeństwo pod maskę trafiłby z pewnością ten pierwszy. A bezpieczeństwo to jedna z najważniejszych przesłanek, którą powinniśmy się kierować, działając w blockchainie.

Podsumowując: NFT to nic innego jak smartkontrakt, który zarządza niewymiennymi monetami (niewymiennymi tokenami). Tokeny te są unikatowe z punktu widzenia własności. To jakby odwrotność normalnej waluty, w przypadku której mówimy, że Jan posiada 100 monet. NFT mówi zaś, że moneta o numerze seryjnym 100 jest w posiadaniu Jana. W kontrakcie każda taka moneta jest precyzyjnie zdefiniowana i po sprzedaży otrzymuje zapis swojego właściciela. Takie monety można dalej odsprzedawać, ale oczywiście pod warunkiem, że się jest ich właścicielem. To dlatego tak ważne jest korzystanie ze sprawdzonego smartkontraktu: żeby osoby trzecie nie mogły wykorzystać potencjalnych dziur i ukraść nam naszych NFT.

NFT oprócz właściciela posiada odniesienie do tego, co reprezentuje. I tu przechodzimy do tych słynnych internetowych obrazków…

Jak już wspomniałem wcześniej, NFT może reprezentować zupełnie tradycyjne przedmioty własności, takie jak samochody czy domy; okazuje się jednak, że token NFT zyskał popularność przede wszystkim dzięki

reprezentowaniu rzeczy wirtualnych: zdjęć, grafik, utworów muzycznych, artykułów, blogów, niewydanych na papierze książek, a nawet zdarzeń, które zaistniały wyłącznie w sieci, a były choć trochę znaczące: należy do nich pierwszy tweet założyciela Twittera, Jacka Dorseya.

Prawo własności a prawo autorskie

Widzisz już pewnie, dokąd to zmierza. NFT może być po prostu cyfrową umową przeniesienia praw własności. W tym miejscu od razu ważna informacja: zauważ, że jeśli NFT reprezentuje zdjęcie znanego artysty, to wyraża tylko tyle, że to zdjęcie kupiłeś i stało się twoją własnością. NFT nie stanowi umowy pozwalającej reprodukować czy komercyjnie używać tego zdjęcia – te działania objęte są standardowym prawem autorskim i podlegają osobnym umowom.

NFT nadaje naszej własności wartość przez jej potwierdzenie – to bardzo ważne, bo w cyfrowym świecie każdy może mieć kopię dowolnego dzieła. Będąc w Luwrze, możemy podjeść do arcydzieła Leonarda da Vinci i zrobić smartfonem zdjęcie *Mona Lisie*, a następnie wykorzystać je na naszych profilach społecznościowych. Nie zmieni to jednak faktu, że tylko Luwr jest właścicielem obrazu. W przypadku *Mona Lisy* sprawa jest oczywista. Jeśli jednak weźmiemy pod uwagę nieprzebrane zasoby sztuki cyfrowej, udowodnienie prawa do własności nie jest już takie proste, szczególnie że łatwość powielania i przechowywania sprawia, że ten sam plik może się znaleźć na wielu dyskach twardych. NFT przychodzi nam z pomocą – to dzięki tym niewymiennym tokenom nie będziemy mieli problemu z wykazaniem, że grafika, która widnieje w naszym awatarze, jest wyjątkowa i kupiliśmy ją od autora. To dzięki NFT nasza grafika staje się

unikatem, mimo że jej kopie mogą krążyć po sieci w niezliczonej liczbie egzemplarzy. NFT honoruje i nabywcę, i autora.

NFT daje artystom nowe możliwości – do swojego dzieła mogą dodać program, który będzie nim niejako zarządzał, na przykład pobierał i przekazywał opłaty licencyjne za jego odtworzenia, wyświetlenia czy za inny sposób konsumpcji treści utworu. Artyści mogą też – dzięki smartkontraktowi – wpływać na to, kto i kiedy kupi ich dzieło, i w ten sposób zapobiegać spekulacjom. Mogą robić to wszystko bez pośrednictwa galerii, operując od razu na swoim kontrakcie NFT. Tworzy to niezależny od instytucji nowy rynek dzieł sztuki.

W takim razie warto zadać pytanie: „Co nabywca może zrobić, a czego nie, z dziełem, które właśnie kupił?”. Skoro zakup dokonał się w blockchainie, trudno sobie wyobrazić, że właściciel dzieła będzie podpisywał osobne umowy o przeniesieniu praw autorskich – na przykład dotyczące ikonki czy awatara. I tu do gry wchodzą wielkie portale aukcyjne, które zajmują się sprzedażą NFT na zasadach licytacji. Pośredniczą między artystami i kupującymi. Standaryzują prawa nabywane wraz z aktem własności NFT. Upraszczają również dostęp do informacji o statusie własności danego dzieła (zwykle jest to link prowadzący do konta nabywcy).

Znudzone Małpy

Rynek NFT bardzo się rozwinął, a same tokeny – choć stuprocentowo wirtualne – zaczęły rządzić się prawami dzieł znanymi ze świata rzeczywistego, nabierając rzeczywistej wartości. Powstały bardzo niszowe portale kreujące kolekcje cyfrowych dzieł NTF.

Najsłynniejsze NFT – te, od których rozpoczął się boom na te cyfrowe produkty – to (między innymi) CryptoPunks i Bored Ape Yacht Club, czyli Klub Jachtowy Znudzonych Małp. Kolekcja Znudzonych Małp to 10 tysięcy unikalnych, przypominających awatary grafik, przedstawiających oczywiście małpy. Mają rozmaite atrybuty: są w czapkach, okularach, hełmach, mogą być ogolone lub nie, czasem są dziwnie ubrane, czasem zupełnie nie mają ubrania. Zawsze jednak są znudzone. Początkowo NFT ze Znudzonymi Małpami sprzedawano po 200 dolarów, ale z biegiem czasu ceny tych grafik – przynajmniej niektórych – mogły sięgnąć setek tysięcy. Wartość dotychczasowej sprzedaży szacuje się na miliard dolarów! Częścią smartkontraktu NFT na Znudzone Małpy jest pełna dowolność komercjalizacji zakupionej grafiki – nabywca może jej użyć na przykład w swojej książce, grafice czy filmie. Sympatycznym bonusem jest dostęp do specjalnego wirtualnego klubu, do którego należą wyłącznie posiadacze tokenów z małpami.

NFT – więcej niż własność

A teraz – zainspirowani Nudnymi Małpami i ich komercyjnym sukcesem – uwolnijmy wyobraźnię… Bo NFT to nie tylko dowód własności, ale także rozmaite funkcjonalności z nim związane.

Bohater otwierającej ten rozdział historyjki jest amatorem szachów i często bierze udział w szachowych turniejach online. Organizuje je jeden z wiodących portali szachowych i nagradza swoich użytkowników tokenami NFT. Z jednej strony stanowią one miłą dla oka pamiątkę, a z drugiej – są kluczem do zalogowania się za darmo do płatnego serwisu. Czyli, innymi słowy, zawierają w sobie abonament!

Pracodawca może szybko zweryfikować autentyczność certyfikatu szkolenia lub dyplomu ukończenia uczelni, jeśli ów certyfikat lub dyplom będą w postaci NFT. Oczywiście w całym procesie osoba starająca się o pracę zachowa – jeśli taka będzie jej wola – pełną anonimowość. W bezpiecznym przekazaniu danych pośredniczy kryptografia: wystarczy, że kandydat na stanowisko podpisze CV tym samym kluczem, którym podpisany jest dyplom lub certyfikat.

Wydarzenia: jubileuszowy koncert lub ważny mecz. Bilety w formie elektronicznej mogą być sprzedawane jako tokeny NFT. Będą one ważne tylko na daną imprezę, a po skorzystaniu z nich mogą stanowić miłą kolekcjonerską pamiątkę, poświadczającą nasz udział w wyjątkowym evencie.

Z zalet NFT mogą skorzystać nie tylko klienci, ale także producenci i sprzedawcy. Znane marki odzieżowe wypuszczają na rynek limitowane kolekcje sygnowane podpisem jakieś znanej osoby – na przykład buty sportowe sygnowane podpisem popularnego koszykarza. Dzięki NFT takie firmy będą mogły rozszerzyć swój zasięg w świecie online. Może uda nam się wywrzeć wrażenie na znajomych, kiedy pierwszy wirtualny mecz w kosza zagramy w butach sygnowanych przez LeBrona Jamesa?

NFT odbudowuje zaufanie w sieci. Blockchain, jako publiczny nienaruszalny zapis transakcji, poświadcza, że dana transakcja na pewno się wydarzyła. Możemy sobie bardziej zaufać.

Wydaje się to wręcz lekiem na instagramowe przekłamywanie świata. Influencerzy nierzadko prezentują się w wypożyczonych samochodach, używają produktów, które wcale do nich nie należą, i wczasują się na opłaconych przez firmy marketingowe wakacjach – wszystko po to, by zwiększać sprzedaż reklamowanych przez siebie produktów i kreować wrażenie, że wszystko dla każdego jest w zasięgu ręki. W zasadzie nie ma

w tym nic dziwnego – tak działa reklama. Ale jest tu pewien kłopot – przez to, że influencerzy nie są w reklamach odbierani jako aktorzy, a jako autentyczni, przeciętni ludzie, mogą przyczyniać się do pewnych problemów społecznych: na przykład podcinać skrzydła młodszym użytkownikom sieci i obniżać ich samoocenę oraz manipulować tymi nieco starszymi.

Problem podprogowego wpływania na użytkowników sieci społecznościowych stał się tak poważny, że Urząd Ochrony Konkurencji i Konsumentów wydał szczegółowe rekomendacje oznaczania treści reklamowych. Jako konsumenci mamy prawo do wiedzy, czy dana treść jest bezinteresowną, wynikającą z osobistych pobudek i doświadczeń oceną produktu, czy opłaconą przez producenta reklamą. Jednak to nie koniec sprawy. Reklamy influencerów są bardzo skuteczne, szczególnie w fandomie, wśród osób, które śledzą ich życie, perypetie, przygody, podróże… Influencerzy budują swoją markę albo w oparciu o ekskluzywność i wysublimowanie świata, w którym się obracają, albo w oparciu o jego niszowość i unikatowość. Jeśli jest to autentyczny obraz, to wspaniale – influencerzy uczciwie pokazują nam cel, do którego sami możemy aspirować. Czy jednak jest on zawsze autentyczny? A może zainscenizowany, wypożyczony, wyleasingowany i na kredyt? Którędy przebiega cienka granica reklamy? Upowszechnienie technologii NFT tak, by była ona częścią produktu, wprowadza tu pełną transparentność. NFT pomoże obu stronom – zapewni pełną wiarygodność. Czy ten dyplom z Oxfordu w tle reklamy nowego szkolenia nie jest przypadkiem certyfikatem ukończenia szkoły letniej? Czy autorki kanałów modowych są właścicielkami zachwalanych kolekcji? A może to zaledwie rekwizyty przekazane przez reklamodawców? Przy pomocy tokenów NFT można bez problemu wszystko udowodnić.

Blockchain, jako platforma zaufania, proponuje nowy wymiar komunikacji w sieci. W sieci, w której nikomu nie możemy zaufać, pojawia się światełko nadziei.

Grzechy NFT

Rynek i technologia NFT są na razie we wczesnym stadium rozwoju. Daje to wiele możliwości, ale pojawia się też sporo zagrożeń.

Wskutek eksplodującego zainteresowania kryptowalutami gigantycznie wzrósł popyt na rozmaite NTF – i to nie tylko na kolorowe obrazki à la Znudzone Małpy, z których wiele sprzedawanych jest po przyprawiających o zawrót głowy cenach (A to wywołuje pukanie się w głowę wśród laików: „Po co tyle płacić za zwykłego JPG-a, skoro za darmo da się go zapisać na własnym dysku”).

Czai się tu wiele niebezpieczeństw.

Jeśli korzystamy z renomowanego serwisu aukcyjnego, który stosuje standardowe smartkontrakty NFT, a podczas zawierania transakcji chronimy klucze prywatne, z technicznego punktu widzenia jakiekolwiek nadużycia stają się mało prawdopodobne.

Dlaczego zatem aż 9 na 10 użytkowników NFT doświadczyło oszustw?

Problemem są ludzie odpowiedzialni za cały ekosystem tworzący, sprzedający i ogólnie utrzymujący NFT, który działa – chcę to wyraźnie podkreślić – poza blockchainem. Ci sami ludzie rozbudzają fałszywe nadzieje na wielkie pieniądze z handlu NFT, chcąc szybko zarobić krocie.

Głównym technicznym problemem jest znikanie serwisów z kolekcjami. NFT – czyli zapisany w blockchainie dowód własności – jest nienaruszony, ale link prowadzący do naszego nabytku nie działa. Strona,

do której prowadzi, przestała istnieć. Twórcy kolekcji nie wywiązali się ze swojej części umowy kupna-sprzedaży.

Czasami sprzedawcy NFT posuwają się do tak bezczelnych oszustw, że stworzony przez nich portal w ogóle nie komunikuje się z blockchainem! Owszem, sprzedają swoje obrazki w serwisie aukcyjnym, ale nie certyfikują ich własności dość kosztownymi transakcjami NFT. Przeciętny kupujący, wmanewrowany w taki zakup, często nie jest niestety na tyle obeznany z zagadnieniem, żeby przyszło mu do głowy, by sprawdzić taki szczegół.

Kolejnym zagrożeniem są standardowe oszustwa kierujące nas do serwisów bliźniaczo podobnych do tych oryginalnych. To technika dobrze znana, żelazny punkt na liście szwindli wyłudzających środki z tradycyjnej bankowości. Tracimy pieniądze, ale nie dostajemy nic w zamian.

Pewnym rodzajem nadużycia, choć o wiele bardziej zniuansowanym, jest aktywność niektórych influencerów w mediach społecznościowych. Promują oni grafiki i kolekcje, które nie mają żadnej wartości artystycznej ani utylitarnej. Nie dysponują żadnym zapleczem, które mogłoby posłużyć do stworzenia żywej społeczności użytkowników danego tokena. Nakręcając sprzedaż, kreują bardzo pozytywną, euforyczną wręcz atmosferę transakcji, ale bezużyteczność tokenów promowanych lub wręcz sprzedawanych przez influencerów to jedno z dziesięciu najczęstszych zażaleń dotyczących NFT. Influencerzy bazują na naiwności i – co gorsza – na oddaniu swoich fanów, którym wmawiają, że w zasięgu ręki jest powtórzenie sukcesu Znudzonych Małp: że na odsprzedaży swoich tokenów za jakiś czas zarobią tysiące procent ich pierwotnej wartości. Niestety, to się nigdy – albo prawie nigdy – nie zdarza.

Skala oszustw związanych z marketingiem fałszywych obietnic przylepiła niesłuszną łatkę naciągactwa całej ze wszech miar pożytecznej branży NFT. Plagą stało się podszywanie pod serwisy z rozmaitymi

kolekcjami lub budzące odrazę sprzedawanie podróbek. Jednocześnie to nic nowego w naszym pięknym kraju (i w sumie w każdym innym). Zobaczymy to szczególnie wyraźnie, jeśli cofniemy się do czasów przemiany ustrojowej, czyli do lat dziewięćdziesiątych XX wieku.

Od NFT do metawersów

Czy pisanie o grzechach NFT nie jest zbyt pesymistycznym zakończeniem poświęconego im rozdziału w książce oswajającej, a wręcz promującej kryptowaluty? Czy to nie jest swego rodzaju strzał w stopę?

Nie wydaje mi się – jestem bowiem przekonany, że to wcale nie koniec. To dopiero początek. Początek wielkiej transformacji, a chyba każda transformacja u zarania przeżywa „okres błędów i wypaczeń". NFT i podobne w działaniu technologie okażą się niezbędne, kiedy nasze życie w dużej części przeniesie się do wirtualnej rzeczywistości, czyli… do metawersów.

Czym w takim razie jest metawersum? Po pierwsze – jest to termin uniwersalny, choć nieco zawłaszczony przez Facebooka, który zmienił nazwę na Meta, by podkreślić, jak ważna dla niego jest migracja do wirtualnej rzeczywistości. Po drugie – pojęcie metawersum pojawiło się po raz pierwszy w powieści popularnonaukowej Neala Stephensona *Zamieć* z 1992 roku. W jej polskim przekładzie metawersum było przetłumaczone jako „metawers" (ja wolę nazwę bardziej kojarzącą się brzmieniowo z „uniwersum" i dlatego jej używam).

Po trzecie – w *Zamieci* metawersum oznaczało wirtualną rzeczywistość, w której bohaterowie utworu Stephensona wiedli drugie, równoległe życie.

No dobrze, ale co mają do tego NFT?

Otóż NFT poświadcza naszą własność… czegokolwiek. A w metawersum trzeba będzie gdzieś mieszkać, czymś się zajmować, w coś się ubrać, a może nawet użyć perfum… Dzięki goglom VR (i być może innym urządzeniom będącym interfejsem łączącym nasze zmysły ze światem wirtualnym) będziemy o wiele głębiej doświadczać tego, co nas otacza. I to wcale nie do granicy, w której rzeczywistość wirtualna będzie nie do odróżnienia od prawdziwej – świat wirtualny może być od niej lepszy: w końcu prawa fizyki, jakie w nim obowiązują, zależą wyłącznie od naszej wyobraźni…

Decentraland to jeden z wielu popularnych projektów metawersów, w których użytkownicy przenoszą się do cyfrowego świata. Wiosną 2022 roku najtańsza parcela w Decentralandzie (kwadrat o boku 16 metrów) kosztowała tam aż 14 tysięcy dolarów! Na takiej parceli może stanąć nasz wirtualny dom, a w nim możemy przechowywać wirtualne kolekcje NFT. Cena parceli jest tym wyższa, im jej położenie jest atrakcyjniejsze: parcele sąsiadujące z ruchliwymi miejskimi arteriami, sklepami i innymi udogodnieniami mają naprawdę wysokie ceny. Łącząc kilka parceli, możemy wznosić wyższe budynki. Decentraland oferuje również kredyty hipoteczne na zakup nieruchomości. Otaczający nas świat, scenę naszej wirtualnej egzystencji, budujemy za pomocą narzędzi Decentralandu – nie musimy umieć programować. W marcu 2022 roku prestiżowa impreza Fashion Week odbyła się także w Decentralandzie – oczywiście w dzielnicy modowej – a jej uczestnikami były wielkie marki, między innymi Dolce & Gabbana, Tommy Hilfiger, Estée Lauder i inne. To wirtualne wydarzenie odbiło się szerokim echem w mediach i jeszcze bardziej zbliżyło nas do migracji do cyfrowej rzeczywistości.

Obecnie matewersa zaczynają charakteryzować się coraz większą specjalizacją. Jedne jako podstawę działania przyjmują parcele, inne

mieszkania w bloku, jeszcze inne – skupiają się na uniwersalnych elementach inwentarza w grach. Osobiście mam nadzieję, że w przyszłości będziemy mogli się poruszać między metawersami różnych firm – będzie to trochę jak przechodzenie między różnymi baśniowymi krainami…

Dla niektórych cały koncept metawersum – czyli połączenia wirtualnej, rozszerzonej rzeczywistości z tą prawdziwą – jest absurdalny i zbyt ulotny: światy wirtualne mogą sprawiać wrażenie nietrwałych, podatnych choćby na przypadkowe wykasowanie czy błędy systemu. Tymczasem tokeny NFT są narzędziem, które może nadać metawersom nieprzemijalność. Byłem bardzo zaskoczony, kiedy przekonałem się, ile pracy włożono w zbudowanie wirtualnych scen – a przecież ludzie muszą wierzyć w trwałość tego, co wytwarzają.

Wszelkie słabości NFT – w tym tanie oszustwa – skończą się, gdy znane firmy wejdą w tę przestrzeń. Gdyby muzyką NFT zarządzał Spotify, to podejrzewam, że w mig zniknęłyby problemy infrastrukturalne, a młodzi artyści otrzymaliby bezpieczną platformę do monetyzacji swoich talentów.

Do nowego świata przeniesiemy dużo naszych słabości – choćby do markowych ubrań czy kolekcjonerskich gadżetów. Przeniesiemy tam również naszą odwieczną potrzebę podkreślania swojej indywidualności i jej nieskrępowanego wyrażania. A NFT będzie technologią, która nam w tym pomoże – na przykład pozwoli zrobić unikalny tatuaż na naszej wirtualnej skórze.

Nowy wirtualny świat będzie również platformą nowej ekonomii dla nadchodzących pokoleń. Nie tylko dlatego, że bardziej zaawansowani wiekiem użytkownicy będą w metawersach mniejszością, ale również przez to, że nie będą dobrze czuli ani rozumieli jej wartości.

Są to idealne warunki do budowania przedsięwzięć i rozwoju. Na początku wirtualnego świata wkładem własnym będzie praca

i pomysłowość. W przeciwieństwie do kapitału, którego młode pokolenie nie posiada, co wyklucza je z tradycyjnych inwestycji.

Od NFT do metawersów. Mam nadzieję, że po przeczytaniu tego rozdziału NFT przestały ci się kojarzyć wyłącznie z małpami, miśkami i tak dalej…

Jak bezpiecznie kupować i sprzedawać NFT?

1. Sprawdź, czy broker lub strona aukcyjna należą do któregoś z największych portali NFT.

2. Czy kupowany przez ciebie NFT istnieje w blockchainie i na jakim smartkontrakcie? ERC-721? ERC-1155?

3. Wielokrotnie sprawdź stronę, do której podłączasz najpopularniejszy portfel przeglądarkowy, czyli metamask. Sprawdź, czy obsługuje protokół https.

4. Czy przedmiot naszego zakupu jest powiązany z jakimś istniejącym metawersum? Czy jest jakkolwiek powiązany z dużymi markami z niewirtualnego świata?

5. Czy NFT, które chcemy kupić, buduje wokół siebie zdywersyfikowaną społeczność, używającą NFT do nauki, zabawy, rozrywki, zarobku, identyfikacji? Społeczności korzystają z wielu platform, takich jak Reddit, Facebook, Twitter, Discord. Czy kupowane NFT możemy śledzić oraz zobaczyć w działaniu choćby w Decentralandzie? Wszystkie te cechy nadadzą użyteczności naszemu NFT i spowodują, że poniesiemy mniejsze ryzyko zakupu pustego tworu.

6. Pamiętaj, że obecnie jeden na trzy projekty NFT kończy się niepowodzeniem.

7. Unikaj NFT wykreowanych przez influencerów tylko dla ich obserwujących. Przekonaj się, jak ich token zachowuje się na rynku poza ich bańką. To pozwoli zweryfikować jego wartość.

8. Jeśli traktujemy NFT wyłącznie jako inwestycję, reguły inwestycji alternatywnych są tu wielokrotnie ważniejsze. Czy kupilibyście unikatowe whisky za istotną część waszych oszczędności na lokalnym straganie?

11

Łańcuch dostaw

„Bzzz, bzzz, bzzz…” Tak dziwnego dźwięku powiadomienia Jan jeszcze nie słyszał.

Rzucił okiem na ekran smartfona i ku swojemu zaskoczeniu zobaczył komunikat aplikacji portfela, którym rano płacił w sklepie spożywczym: „Ważne! Prosimy o utylizację produktu: »szynka krojona ze spichrza«. Podejrzenie salmonelli”.

Złote czasy i krwawe diamenty

Zanim przejdziemy do głównego tematu rozdziału, przenieśmy się do roku 2017. Moje mimowolne skojarzenie z tego czasu to pierwsza gigantyczna fala wzrostu kursów kryptowalut i rozpisujące się o niej media głównego nurtu. Nowe kryptowaluty wzbijają się na kilkusetprocentowe szczyty, co przyciąga do nich zaskakujących graczy: korporacyjni giganci, tacy jak IBM czy Hewlett-Packard, nagle pragną uczestniczyć w, było nie było, anarchistycznej platformie. Istne zderzenie dwóch zupełnie odmiennych światów. Ale czy na pewno aż tak odmiennych? Czy „anarchistyczne” rozwiązania i narzędzia świata kryptowalut nie mogą być – paradoksalnie – wykorzystane komercyjnie?

Oczywiście, że mogą – a nawet powinny! Blockchain nadaje się wprost idealnie do ochrony prywatności, zarządzania dostępem do danych i do ich analizy. Blockchain to przecież taka publiczna księga. Zawiera mnóstwo cennych, choć zupełnie anonimowych informacji, które można wykorzystać dla szeroko pojętego ogólnego dobra.

Rozwój kryptowalut przebiegał bardzo dynamicznie. Prowadzono dużo badań, pojawiły się znaczne budżety umożliwiające powstanie rozmaitych prototypowych rozwiązań i zaczęto organizować najzupełniej komercyjne konferencje, zapraszając na nie przedstawicieli świata wielkich korporacji.

Na tych niezwykle owocnych i inspirujących konferencjach z reprezentantami środowiska biznesu spotykali się przedstawiciele nauki i techniki. Wyobraźcie sobie tylko tę synergię! Niektóre z konferencji na zawsze zapisały się w mojej pamięci – i to nie tylko przez rozmach, jaki im towarzyszył, ale także, a może przede wszystkim, dzięki okazji bezpośredniej rozmowy z twórcami wczesnych kryptowalut. Wtedy byli żołnierzami na pierwszej linii frontu – często jednocześnie pisali kod swoich genialnych rozwiązań informatycznych i artykuły naukowe do specjalistycznych magazynów. Dziś są sławni i trudno dostępni: ich profile społecznościowe są zarządzane przez firmy marketingowe, a nazwiska poprzedza łańcuszek tytułów naukowych i skrótów korporacyjnych stanowisk.

Jednak po którejś z kolei konferencji, której główny wykład miał dotyczyć zastosowań blockchaina, nie mogłem powstrzymać uśmiechu… zrezygnowania. Dlaczego? Bo po raz kolejny roztoczono w jego trakcie zupełnie niepraktyczne i niepragmatyczne wizje, których ukoronowaniem było „zarządzanie łańcuchem dostaw” (*Supply Chain Management*). Z jakiegoś przedziwnego powodu to wykorzystanie blockchaina zawsze ilustrowano… tym samym zdjęciem diamentów! Wyświetlany przy nim

slogan głosił, że oto blockchain rozwiąże problem „krwawych diamentów” – czyli diamentów pochodzących z nieznanych źródeł, a w rzeczywistości głównie z afrykańskich kopalni znajdujących się na terenach objętych działaniami wojennymi; dochód z handlu tymi diamentami finansuje wojny i rozlew krwi, stąd nazwa.

I wtedy zacząłem się zastanawiać… Czy rzeczywiście ukrócenie nielegalnego handlu diamentami jest jedynym wartym wymienienia zastosowaniem kryptowalut w zarządzaniu łańcuchem dostaw? Oczywiście, że jest to ważny problem, a jego etyczne aspekty nie do pominięcia, tyle że nie dość, że już dawno wprowadzono stosowne i skuteczne rozwiązania, to jeszcze nielegalne kopalnie są od dłuższego czasu w niełasce światowych kupców. Może więc jednak skupmy się na tym, jak nasze codzienne życie zyska na zastosowaniu blockchaina do zarządzania łańcuchem dostaw?

Łańcuch dostaw

Zacznijmy od tego, czym tak naprawdę jest łańcuch dostaw. Otóż jest to sieć powiązań pomiędzy firmami, producentami, usługodawcami i dostawcami, której celem jest dostarczenie końcowego produktu do rąk klienta. Takie powiązania obejmują pozyskanie lub wydobycie surowych materiałów, ich przetworzenie, uzdatnienie, obróbkę, stworzenie półproduktów, ich ostateczne zmontowanie, by mogły stać się produktem docelowym, który trzeba następnie zaoferować i dostarczyć klientowi.

Jak najlepiej przekonać się o wpływie łańcucha dostaw na nasze życie? Na przykład możemy spojrzeć na etykietę dowolnego produktu w sklepie spożywczym… Ot, choćby na rybę zapakowaną w folię. Pochodzi z Tajlandii, więc zanim trafiła do sklepowej zamrażarki, musiała przebyć

daleką drogę. Została wyłowiona, oczyszczona, zamrożona i przetransportowana… Mamy nadzieję, że to wszystko odbyło się w takiej właśnie kolejności. No i by się w tym utwierdzić, możemy skorzystać z narzędzi służących do zarządzania łańcuchem dostaw.

Trudno w to uwierzyć, bo przecież mamy XXI wiek i wszystko powinno być w pełni zinformatyzowane, ale wgląd w dane dotyczące ogniw łańcucha dostaw jest bardzo ograniczony. Wynika to z trudności w komunikacji pomiędzy poszczególnymi podwykonawcami, stosowaniu różnych formatów zapisów, a nawet używania papierowej i niedigitalizowanej dokumentacji…

Jak nietrudno się domyślić, jest to źródło wielu problemów. Firmy spedycyjne szacują, że błędy w opisie przesyłek dotyczą aż kilkunastu procent ich tranzytu. Producenci artykułów spożywczych oceniają, że przekłamania informacyjne dotyczą około 40% co bardziej złożonych produktów. Takie nieprawidłowości skutkują nie tylko codziennymi problemami z logistyką (niedostarczone przesyłki, popsuta żywność i zwiększone koszty), ale także wprowadzają klienta w błąd. Nie mamy pewności, skąd pochodzą półprodukty, nie wiemy, jakie z nich zawiera nasz towar ani czy do ich pozyskania lub produkcji nie wykorzystano dzieci lub czy nie pochodzą z rejonów świata o wątpliwej czystości środowiska.

Chyba już widzisz, że szczytna, choć nieco wyświechtana wizja zastosowania blockchaina do śledzenia diamentów od kopalni aż do pierścionka może mieć znacznie szersze i praktyczniejsze przełożenie.

Na ratunek wizerunkowi

Walmart. To taki odpowiednik Biedronki w Stanach Zjednoczonych, tylko że znacznie od niej większy. Firma większa ekonomicznie od niejednego państwa, warta niemal czterysta miliardów dolarów (to czteroletni budżet Polski). W 2017 roku rozpoczął wdrażanie śledzenia łańcucha dostaw żywności. Dlaczego Walmartowi tak zależało na kontroli łańcucha dostaw? Bezpośrednia przyczyna to zatrucia spowodowane spożyciem sprzedawanego w sieci sklepów zepsutego jedzenia. Kiedy przyszło co do czego, Walmart nie był w stanie prześledzić, kto i gdzie odpowiada za wadliwy produkt, nie mógł też ustalić, jak duża jest skala problemu i z których sklepów produkt należy wycofać. Na jakim etapie produkcji jedzenie się popsuło i dokąd zostało wysłane? Czy wiozła je jedna ciężarówka chłodnia obsługująca kilka miasteczek, czy może ekspediowana była z centralnego magazynu dystrybucyjnego? A może zapewnił je lokalny dostawca? Niekompletna dokumentacja sieci dostawców bez funkcjonalności wglądu w dane i brak dokumentów w formie papierowej sprawiły, że Walmart okazał się bezradny wobec wewnętrznego kryzysu. Kryzysu, który stanowił realne zagrożenie dla zdrowia klientów sieci, a dla niej samej był istną katastrofą wizerunkową.

Walmart zaczął szukać rozwiązania, które zapobiegnie podobnym problemom w przyszłości. W końcu zarządzanie swoim łańcuchem dostaw przeniósł do blockchainu, który – jako wspólna baza danych – standaryzuje komunikację wszystkich współpracujących ze sobą podmiotów. Można w niej natychmiast prześledzić działania dostawców każdego oferowanego produktu. Przy użyciu odpowiednich narzędzi i skanerów z łatwością dociera się do informacji, kto dostarczył półprodukty, jak zostały przetransportowane i skąd dokąd. I wszystko to może się odbyć w anonimowy sposób, choć zwykle w takich systemach anonimowość jest

jednostronna: dostawcy nie mają wglądu w łańcuch dostaw, za to zamawiający dysponuje dostępem do kompletnych informacji.

Dostawy żywności, podobnie jak wszelkich innych produktów, można skutecznie monitorować. Część danych możemy udostępnić producentom i przewoźnikom, aby mogli na bieżąco dostosowywać do zapotrzebowania swoje moce produkcyjne i dostępność floty. Zmniejsza to koszty i zwiększa bezpieczeństwo.

Jeśli sprzedawcy zależy na pełnej transparentności, wszystkie te dane może udostępnić również kupującemu. Nic nie stoi na przeszkodzie, by skanując kod kreskowy, klient zyskał pełną informację o drodze, jaką przebyła ryba, którą kupił na dzisiejszy obiad. Pełną informację: nie tylko skąd wyruszyła, ale jak długo trwał każdy z etapów jej podróży. Dane te są osiągalne w bazie blockchaina, którą da się łatwo zweryfikować.

Blockchain wyróżnia się architekturą: został od podstaw zaprojektowany tak, by służył do współpracy i zawierania umów. A to sprawia, że w blockchainie wszyscy musimy (i chcemy) rozmawiać w tym samym języku.

Przytoczę jeszcze kilka przykładów zastosowania blockchaina w zarządzaniu łańcuchem dostaw, na które trafiłem przy różnych okazjach mojej kryptowalutowej pracy (i pisania tej książki).

Żywność

Okazuje się, że połączenie inteligentnych czujników IoT (*Internet of Things*, internet rzeczy) i blockchaina może wygenerować naprawdę dużo wartościowych danych. W krajach południowo-wschodniej Azji wiele

uwagi poświęca się jakości mięsa. Wyobraź sobie, że… jest ono często podrabiane! Zdarza się to w dwóch typach przypadków.

Pierwszy z nich to sytuacja, kiedy nieuczciwy kontrahent próbuje sprzedać mięso, zwykle wołowinę, „z prestiżowych farm i z najcenniejszych zwierząt", choć oczywiście jego towar wcale z nich nie pochodzi. Jeśli cały proces produkcji mięsa obejmiemy monitoringiem z zastosowaniem czujników sprzężonych z blockchainem, wciśnięcie klientom tak fałszywie opisanego mięsa stanie się bardzo trudne. W każdej chwili da się bowiem sprawdzić, jaka ilość mięsa została wyprodukowana i ilu odbiorców potwierdziło jego zakup. Może się to odbyć z pełnym poszanowaniem prywatności, i to zupełnie dobrowolnie. Kupujący sami – anonimowo! – rejestrują swój akt odbioru w imię ogólnego dobra, by walczyć z podróbkami (czy niezgodnymi z prawdą deklaracjami).

Druga sytuacja, która może być źródłem oszustw, dotyczy samej produkcji. Wówczas pochodzenie mięsa może być prawdziwe, ale sam proces jego wytwarzania może odbiegać od wyśrubowanych norm, za których przestrzeganie płaci przecież odbiorca. Możemy zatem wyposażyć linię produkcyjną w rozmaite czujniki, choć większość z nich jest już zautomatyzowana i zawiera potrzebne urządzenia wejścia/wyjścia (wagi, urządzenia kontroli dostępu pracowników, kamery, skanery i tym podobne). Po zintegrowaniu takich czujników w jedną platformę możemy łatwo dowieść, że mięso spełnia założone normy produkcji. Taka kontrola – oprócz zapewnienia pożądanej jakości produktu – ogranicza też zagrożenie epidemiczne.

Przenieśmy się w rejon nieco innych smaków. Awokado. Bardzo zdrowy owoc. I bardzo drogi. A z racji niekorzystnego wpływu na środowisko (wycinki lasów pod uprawy, wyjałowienie gleb przez monokulturę) – dość kontrowersyjny. Doczekał się jednak swojego

własnego blockchaina, który zwie się po prostu… Avocado Chain. Ten blockchain został stworzony w szczególności po to, by dokumentować, czy „produkcja” i transport awokado są zgodne z zasadami Fair Trade. Taki etyczny wymiar handlu jest bardzo ważny także w przypadku wydobycia metali ziem rzadkich oraz w handlu drewnem egzotycznym. Szacuje się, że nawet połowa egzotycznego drewna może pochodzić z nielicencjonowanych, rabunkowych wyrębów.

Leki

Śledzenie łańcucha dostaw ma kapitalne znaczenie w transporcie półproduktów wykorzystywanych w przemyśle farmaceutycznym. Często przesyłane są one w kontenerach morskich, które przemierzają długą drogę między odległymi miejscami, na przykład między Japonią a Szwajcarią (oba kraje to duże ośrodki przemysłu farmaceutycznego). Transport musi odbywać się w ściśle określonych warunkach (wilgotność, temperatura i tym podobne) – dopiero wówczas mamy gwarancję, że zawartość, która dotrze na miejsce, będzie nadawała się do dalszych etapów produkcji. Warunki transportu monitorowane są czujnikami temperatury i wilgotności, które nadawca umieszcza w pudłach z półproduktami. Szkopuł w tym, że czujniki te przesyłają dane do… nadawcy. Odbiorca musi więc wykazać się nie lada zaufaniem, przyjmując od nadawcy raport niezawierający danych z transportu półproduktów. Zintegrowanie czujników ze współdzieloną platformą, jaką jest blockchain, rozwiązałoby kwestię zaufania. Nie dość, że obie strony miałyby wgląd w tak kluczowe dane, to w razie jakichkolwiek problemów można tym danym bezwarunkowo zaufać:

wykluczona jest tu jakakolwiek zmiana wpisów odczytu czujników, i to przez którąkolwiek ze stron.

Producenci i administracja państwowa

A czy blockchain mógłby usprawnić komunikację między firmami a administracją rządową? Oczywiście! Najlepszym przykładem są wszystkie te dziedziny aktywności gospodarczej (i nie tylko gospodarczej), które wymagają ścisłego zarachowania. Jako przykład omówmy… uprawę konopi indyjskich.

Choć w Polsce ma być dopiero zalegalizowana, na świecie jest to już gigantyczny przemysł. Zastosowanie kryptowalut i blockchaina do jego obsługi to coś, co ułatwia życie zarówno regulatorowi (państwu), jak i producentom. Regulator, stosując opisane powyżej mechanizmy, ma wgląd w linię produkcyjną, ilość wyprodukowanego towaru, a nawet tożsamość pracowników. Producent – za pośrednictwem tych samych mechanizmów – może ściśle kontrolować jakość otrzymywanego produktu, porównując jego partie i identyfikując lepszych i gorszych dostawców surowego produktu. Sam proces produkcji suszu jest niesłychanie złożony. Suszenie, mielenie, transport – to wszystko musi się odbywać w określonym czasie i określonych temperaturach. Maszyny między partiami muszą zostać oczyszczone. Oprogramowanie może odegrać tu kapitalną rolę w podnoszeniu jakości. I tak dochodzimy do odbiorcy, który może wybrać tego producenta, który zechce podzielić się z nim informacją o pochodzeniu i szczegółach obróbki konopi.

Na szczeblu samorządowym możemy zastosować zupełnie inny aspekt zachęt producenckich. Kontrolując pochodzenie płodów rolnych, możemy

na przykład zachęcać lokalne restauracje i stołówki do korzystania z produktów wytworzonych na miejscu. Wszyscy zainteresowani nie tylko mogą sprawdzić pochodzenie składników potraw – również wymiana handlowa może odbyć się za pomocą lokalnej waluty. Oczywiście taka procedura musi zostać najpierw uregulowana przez ustawodawcę. Blockchain stanowi niesamowite narzędzie rozwoju regionalnego.

Oprogramowanie

Na zakończenie tego rozdziału, w którym omawialiśmy zarządzanie łańcuchem dostaw za pomocą blockchaina, chciałbym ci pokazać zupełnie nieoczekiwaną w tym kontekście dziedzinę naszego życia. Chodzi mi o software: programy, które sprawiają, że nasze komputery, konsole do gier i… sieci społecznościowe zaczynają tętnić życiem.

Pewnie się dziwisz, bo cóż wspólnego może mieć transport półproduktów na kontenerowcach z pisaniem kodu programu? Otóż więcej, niż się spodziewasz. Przecież oprogramowanie też tworzy się z półproduktów. Łańcuch dostaw w przypadku oprogramowania to tak zwany manifest, na który składają się wszystkie podprogramy i podsystemy, wymagane do działania tworzonego programu.

W maju 2021 roku prezydent USA Joe Biden zarekomendował tworzenie manifestów łańcucha dostaw do oprogramowania w rozporządzeniu wykonawczym numer 14028, którego celem było podniesienie państwowego poziomu cyberbezpieczeństwa. I już niedługo po tym mogliśmy się przekonać, że wiedzy o składnikach, z których przyrządzamy naszą informatyczną zupę, nie można nie doceniać.

W grudniu 2021 roku ujawniono, że log4j – darmowa biblioteka języka Java, wykorzystywana w olbrzymiej większości oprogramowania tworzonego na całym świecie – ma w swoim kodzie krytyczny błąd, który pozwala na wykonanie dowolnej instrukcji poza jakąkolwiek kontrolą twórców i operatorów systemów. Wywołało to nie lada panikę w świecie informatycznym. Tuż przed świętami Bożego Narodzenia programiści zaczęli wymieniać się w swoich grupach roboczych setkami e-maili oznaczonych jako priorytetowe. Zawierały one pytania: „Co to jest log4j?", „Czy używamy tej biblioteki?", „W których programach?", „Czy można nas zhakować?". Tymczasem odpowiedzi na wszystkie te pytania mógłby zawierać blockchainowy manifest obsługujący łańcuch dostaw oprogramowania.

Fake newsy

Rozdział o zarządzaniu łańcuchem dostaw za pomocą blockchaina chciałbym zamknąć tematem bliskim każdemu z nas. Fake newsy i clickbaity. Słyszał o nich każdy – przecież praktycznie wszyscy korzystamy z mediów: tych „klasycznych" (telewizja, gazety, radio) i tych współczesnych (portale internetowe, media społecznościowe, podcasty i sieciowe materiały wideo). I podejrzewam, że nieraz padliśmy ich ofiarą! Więcej: podawaliśmy je dalej, przyczyniając się do szerzenia nieprawdy.

Szczególnie media internetowe są w stanie bardzo tanio i bardzo łatwo „wyprodukować" albo bardzo kontrowersyjne, albo wręcz nieprawdziwe treści. Krzykliwe nagłówki niezdradzające szczegółów artykułu (clickbaity – *bait* to w języku angielskim „przynęta") zachęcają do kliknięcia w link i przeczytania rzekomo sensacyjnej treści, po czym

okazuje się, że ta treść to tylko lanie wody i podkręcona, przekoloryzowana interpretacja najzwyklejszego pod słońcem wydarzenia, które normalnie nie przykułoby niczyjej uwagi. Pół biedy, jeśli przynajmniej jest ono prawdziwe! Problem z fake newsami i clickbaitami, jak pewnie dobrze wiesz, polega na tym, że sensacyjne i kontrowersyjne przekazy rozpowszechniają się w sieci szybciej i skuteczniej niż „nudne" prawdziwe wiadomości, co jest bardzo często wykorzystywane przez propagandę (tu polecam świetną książkę *Mindf*ck* Christophera Wyliego).

Po części wynika to z ułomności natury człowieka, a po części z funkcjonującego w sieci ułomnego w wielu aspektach modelu biznesowego. Im więcej kliknięć, tym więcej reklam. Im więcej reklam, tym większy dochód. A że w internecie nie lubimy za nic płacić, sami stajemy się towarem i przekaźnikiem fake newsów i clickbaitów.

Czy moglibyśmy zastosować blockchainowy łańcuch dostaw w odniesieniu do internetowych przekazów informacyjnych? To trudne zadanie… Ja wyobrażam to sobie jako drobne wzbogacenie interfejsu użytkownika. Obok tytułu newsa wyświetlałaby się punkty rankingowe wyliczane na podstawie liczby i znaczenia źródeł, z których korzystał autor artykułu. Konwencja byłaby taka, że im więcej punktów widniałoby przy artykule, tym byłby on bardziej wiarygodny – w sensie: lepiej sprawdzony. Słowem: dla każdego newsa prezentowana przy jego tytule liczba byłaby swoistym rankingiem wiarygodności (do jej wyliczania można by jeszcze użyć osobistego rankingu wiarygodności autora i medium, dla którego ów autor pracuje). Jak taki mechanizm mógłby zapobiegać fakenewsowym oszustwom? No i dlaczego którykolwiek portal w ogóle chciałby używać takiego narzędzia?

Cóż, wszystko zależy od nas. Jeśli przestalibyśmy korzystać z niesprawdzonych informacji, to dość szybko każdy serwis dążyłby do

wdrożenia takiego rozwiązania. Jeśli opierałoby się ono na blockchainie, autor artykułu mógłby dokładnie wskazać zapisane w nim źródła, z których korzystał. Blockchain jest otwartą platformą. Każdy twórca mógłby z niej korzystać. Poza tym moglibyśmy do rozliczeń na blockchainie zaprosić samych reklamodawców. Może byliby skłonni premiować wiarygodne treści w imię podnoszenia wiarygodności zawartych w swoich przekazach haseł reklamowych ?

Newsy, fake newsy, clickbaity, szybsze roznoszenie się sensacyjnych, fałszywych treści to temat rzeka i zagadnienie na pograniczu psychologii, inżynierii społecznej, informatyki i… niestety polityki. Mam jednak wrażenie, że blockchain – jako weryfikowalne źródło prawdy – mógłby pomóc w ulepszeniu tego aspektu naszego wirtualnego życia.

Łańcuch łańcucha dostaw

Mam nadzieję, że temat łańcucha dostaw przybliżył ci kolejne zalety blockchaina i nowe możliwości zastosowania technologii kryptowalutowych w codziennym życiu. Otwartość blockchaina sprawia, że obszary, w których ludzie i firmy mają trudności z wzajemną komunikacją i wymianą (prawdziwych) informacji, mogą szybko się skurczyć. Z korzyścią dla naszego zdrowia, środowiska i… kieszeni!

12

Zdrowie

Pieszy został potrącony na przejściu. Co chwilę traci przytomność. Szok na moment wymazał mu pamięć, w dodatku mężczyzna nie rozumie, co mówi do niego ratownik medyczny, który pyta o kontakt z rodziną i grupę krwi…

– Sprawdź jego telefon, może ma token na obudowie!

– Jest!

– Przyłóż do terminala SOR-u! To kryzysowa sytuacja, jesteśmy uprawnieni do odczytania danych. Sprawdź przez ID pacjenta, jaką ma grupę krwi. Sprawdź, czy udzielił stosownych zgód.

„Czy respirator mnie słyszy?”, czyli wymiana danych

Ochrona zdrowia to bardzo ważna dziedzina życia, a zarazem bardzo szeroka: przenikają się tu medycyna, informacje i finanse (ubezpieczenia, koszty zabiegów oraz finansowanie placówek medycznych).

Nas w tej książce najbardziej będą interesowały informacje: przyznasz, że od ich aktualności, kompletności i szybkości przekazywania w odpowiednie miejsca zależy stan zdrowia pacjenta. Dane dotyczące zdrowia są zatem niezwykle istotne. Tymczasem w obecnym systemie

ochrony zdrowia nie ma zunifikowanej platformy, za pomocą której można by nimi skutecznie zarządzać.

Zwykle jest tak, że rejestrujemy się w odpowiadającym naszemu problemowi zdrowotnemu punkcie medycznym, gdzie przebiega nasza diagnoza i leczenie, a ów punkt wydaje nam wyniki badań, opisy specjalistów i skierowania do kolejnych punktów. Niestety pacjent potem zostaje pozostawiony sam sobie: wszystkie dane pochodzące z leczenia lub diagnozy zapisywane są na raczej starożytnych wynalazkach, takich jak płyta DVD, lub przesyłane w postaci załączników (często skanów) do e-maili. Kiedyś odejście od papieru i teczek wypełnionych dokumentacją może i było przełomowe, lecz obecnie takie rozwiązania są dość odległe od pożądanego scenariusza obiegu danych. Do tego wszelkie nasze dane zdrowotne są przechowywane w systemach niezależnych firm medycznych, co rodzi kolejne problemy. Po pierwsze, zwykle nie wiemy, jak długo będą przechowywane nasze dane i jaki owe firmy zapewniają im poziom bezpieczeństwa. Po drugie, mimo że większość portali punktów medycznych jest przyjazna i oferuje nam dostęp do naszych danych online, brakuje łączności pomiędzy nimi – nie da się w pełni automatycznie przekazać naszych wyników między dwiema placówkami, co bardzo często bywa konieczne.

Brak ustandaryzowanego systemu komunikacji i wymiany danych ma poważne konsekwencje.

Pierwsza z nich to brak łączności z urządzeniami medycznymi. Choćby z dializatorami (sztucznymi nerkami), które używają kart pamięci. Ze względu na ich ograniczoną pojemność lekarz odpowiedzialny za ich obsługę nie ma pełnego dostępu do wszystkich pożądanych informacji w każdej chwili. Trudno też o możliwość agregacji i analizy danych, takich jak choćby wyniki badań krwi i wyniki dializ, nie mówiąc już nawet

o interaktywnym dostrajaniu pracy urządzenia na podstawie wyników badań dostarczanych z zewnątrz.

Drugi problem ujawnia się w nagłych przypadkach, kiedy szybki dostęp do danych dotyczących zdrowia pacjenta bywa czasem kwestią życia i śmierci, a brak takiego dostępu w najlepszym przypadku niebezpiecznie opóźnia konieczną pomoc medyczną.

W mniej dramatycznych przypadkach wybrakowane, niekompletne lub zagubione dane to strata czasu i pieniędzy, gdyż może to oznaczać konieczność powtórzenia nierzadko kosztownych badań.

Nie są to nowe problemy; wiele krajów zaczyna już wdrażać stosowne systemy informatyczne. Niestety, w większości z nich dane wciąż pozostają wyizolowane – nie ma pełnej łączności między wszystkimi możliwymi komórkami opieki zdrowotnej (w tym urządzeniami medycznymi). Dzieje się tak z powodu niedoskonałej interoperacyjności systemów. Ich elementy nie potrafią się ze sobą dogadać już na poziomie technicznym, a surowe prawo ochrony danych osobowych nie motywuje – mówiąc oględnie – do ich usprawniania pod tym kątem.

Kryptoportfel zdrowia

Nie bez przyczyny zarysowałem obraz systemu ochrony zdrowia z perspektywy obiegu danych i pokazałem jego mankamenty w tym aspekcie. Zapewne domyślasz się, dlaczego to zrobiłem i co mogłoby być doskonałym antidotum na wspomniane bolączki. Tak – blockchain. Blockchain, który w rdzeniu opiera się na współpracy między wieloma węzłami sieci, przychodzi z gotowym rozwiązaniem. Pełna wymienność i dostępność danych to zresztą tylko jedna z dwóch bardzo ważnych zalet

tego narzędzia w kontekście medycznym. Drugą jest pełnia władzy nad swoimi danymi, z której wprost wynika wysoki poziom bezpieczeństwa prywatności (i anonimowości) pacjentów.

Blockchain to platforma, na której pacjent ma całkowitą kontrolę nad tym, jakie dane udostępnia i komu, gwarantująca jednocześnie ich nienaruszalność i trwałość. Aplikacja, która służyłaby do obsługi medycznego blockchaina, byłaby swego rodzaju kryptoportfelem zdrowia – mogłaby prezentować podstawowy profil zdrowotny pacjenta na badaniach i logować go do urządzeń medycznych, udostępniając im stosowny zestaw jego danych. Urządzenia medyczne (służące do diagnostyki lub leczenia) wysyłałyby dane do współdzielonej bazy danych – czyli medycznego odpowiednika kryptowalutowego blockchaina. Lekarz miałby do nich bieżący dostęp – ale tylko pod warunkiem zgody pacjenta. Tylko pomyśl, jakie byłyby tego zalety! Analiza danych zdrowotnych konkretnego pacjenta mogłaby zupełnie automatycznie wpływać na parametry podłączonego do blockchaina urządzenia, choćby wspomnianego już wyżej dializatora, i to nie tylko w czasie konsultacji, które odbywają się zwykle co kilkadziesiąt zabiegów. Urządzenie – dzięki wymianie danych za pośrednictwem blockchaina – mogłoby działać optymalnie niemal cały czas!

Prywatność w blockchainie wynika z precyzji w wyodrębnianiu konkretnych zaszyfrowanych danych. W medycynie ta precyzja przełożyłaby się z pewnością na mniej błędów wynikających z pomyłek w dokumentacji czy z niekompletnych wyników badań (jeśli interesują cię błędy medyczne, ich źródła i konsekwencje, koniecznie przeczytaj wstrząsającą – i oświecającą – książkę Matthew Syeda *Metoda czarnej skrzynki*). Ponieważ każdy zestaw danych musi być popisany kluczem

pacjenta, oprogramowanie dowolnego punktu medycznego zawsze jest w stanie zweryfikować ich autentyczność i kompletność.

Pełna prywatność i kontrola nad osobistymi danymi medycznymi – poniekąd paradoksalnie – rozwiązuje problem zderzenia się dwóch skrajności: nagłej konieczności leczenia i powolnej machiny biurokratycznej. W naszym kryptoportfelu zdrowia możemy zadeklarować, do jakich danych ma dostęp służba ratownicza podczas zdarzenia lub natychmiast po nim, a jakie spośród nich wymagają zgody na przykład członka rodziny. Napisałem „na przykład”, bo powinowactwo nie byłoby tu prawnie konieczne: dane odblokowuje dowolna osoba, którą zarejestrujemy w naszym medycznym smartkontrakcie. Jej klucz prywatny pozwoli na dostęp do naszych danych niezależnie od tego, czy to nasz mąż, dziewczyna czy po prostu współlokator.

Biurokracja kontra kryptokracja

Kolejny aspekt dobrodziejstw ochrony naszych danych osobowych przez blockchain i kryptografię ujawnia się w kontekście rozmaitych procedur biurokratycznych, które wymagają zaprezentowania wyników konkretnych badań lekarskich przy staraniu się o pracę w specyficznych zawodach. Dzięki blockchainowi pracodawca otrzyma dowód, który niepodważalnie potwierdzi, że nasze predyspozycje zdrowotne wpadają w wymagane przez niego zakresy, ale nie pozna dokładnych wyników badań. Nie dowie się na przykład, jaki lekarz nas badał i czy nie diagnozowaliśmy jeszcze czegoś innego. Jedyne, co zostanie mu udostępnione, to wymagane certyfikaty zgodności.

Pseudoanonimizacja danych medycznych, czyli swego rodzaju oddzielenie ich od właściciela przy jednoczesnym zachowaniu ich niepodważalnego przypisania do niego, sprzyja pacjentom również z finansowego punktu widzenia. Ot, choćby taki ubezpieczyciel… W przypadku chęci skorzystania dokumentacji medycznej swojego klienta, nie mógłby żądać bardziej szczegółowych danych, niż pozwala na to prawo. Oferta ubezpieczyciela będzie musiała oprzeć się na precyzyjnym zestawie informacji, o które nas on poprosi, i nic ponadto. Mówiąc kolokwialnie: „nie będzie miał na nas niczego innego”. Wyeliminuje to jakąkolwiek dyskryminację ze względu na stan zdrowia.

Obecnie problemy pacjentów są często związane z uczestnictwem w komercyjnych badaniach genetycznych. Szczególnie dotyczy to USA, gdzie wyniki takich badań nie są chronione prawnie tak, jak dane medyczne. Jeśli ubezpieczalnia pozyskałaby w jakiś sposób informacje o naszym DNA lub choćby o DNA naszych krewnych, mogłaby zmienić warunki polisy lub całkowicie odmówić jej wydania z uwagi na odkryte w kodzie genetycznym ryzyko chorób.

Z aptekarską precyzją

Gigantyczną częścią systemu opieki zdrowotnej jest oczywiście farmacja. Myślę, że już poprzedni rozdział (o zarządzaniu łańcuchem dostaw) unaocznił ci przydatność blockchaina w tej dziedzinie. Rozwińmy to trochę.

Dzięki blockchainowi pacjent mógłby bardzo szybko wykryć niestandardowe, podejrzane pochodzenie leków lub samodzielnie potwierdzić deklarowaną kompatybilność zamienników. Gdy wiedza o tym, że możemy zażądać od producenta informacji o pochodzeniu każdego leku

czy urządzenia i za pośrednictwem blockchaina łatwo je zweryfikować, przebije się do świadomości publicznej, liczba pseudonaukowych oszustw znacznie spadnie. Lekarz będzie mógł zalecić starszym pacjentom, by nie kupowali żadnych specyfików, których nie ma w oficjalnych medycznych bazach danych. Zaoszczędzi to nam wielu dramatów wynikających ze zmanipulowania starszych pacjentów przez nieuczciwych sprzedawców. Kiedy każdy z nas będzie w stanie skontrolować łańcuch dostaw surowców i produktów, wszyscy łatwo się przekonają, że „magiczny strukturyzator wody" za kilka średnich krajowych wytwarza… najzwyklejszą wodę.

Na koniec przytoczę dwa nieoczekiwane benefity kryptowalutowego podejścia do zdrowia. Pierwszy z nich to rozwój nauki. Blockchain zawiera zanonimizowane dane zdrowotne i jest ich – statystycznie rzecz biorąc – bardzo dużo. To oznacza, że bez naruszania prywatności i bez tej całej biurokracji związanej z koniecznością udzielania zgód na wykorzystanie informacji o zdrowiu będzie można wykorzystać je w badaniach na uniwersytetach i w instytutach. Koszt badań w związku z tym znacząco spadnie, poprawi się ich statystyka, co w konsekwencji doprowadzi do zwiększenia skuteczności leków i procedur medycznych. Wszyscy zyskamy.

Na froncie walki z pandemią

Gdy piszę o zastosowaniu blockchaina w medycynie, wygaszane są ostatnie obostrzenia pandemiczne, na co – po trudnych latach 2020–2022 – wszyscy czekali z utęsknieniem. Pandemia COVID-19 zmieniła nasze życie i nas samych. Jednym z przykrych elementów epidemicznej codzienności była dezorganizacja życia przez kwarantanny. Złożoność problemu powodowała,

że przepisy o tym, kto się kwalifikuje do kwarantanny, a kto i kiedy ją kończy, były czasem niezrozumiałe, a wręcz zaskakujące. W wielu krajach, w tym w Polsce, z prośbą o pomoc zwrócono się do komercyjnego sektora rynku IT. Dość szybko powstała aplikacja, która jako dowód przestrzegania kwarantanny przesyłała zdjęcia danej osoby z informacją o lokalizacji i czasie. Dla mnie osobiście dość dużym problemem były nieznane losy wysyłanych danych. Przecież to były prywatne zdjęcia, na tle mojego domu, z dokładnie podanymi współrzędnymi geograficznymi. Co się z nimi działo? Gdzie były przechowywane? Przez kogo? Jak długo? Czy były zaszyfrowane?

Gdyby u podstaw tego systemu weryfikującego kwarantannę znalazł się blockchain, nie miałbym tylu wątpliwości i nie obawiałbym się potencjalnych zagrożeń naruszenia mojej prywatności. Za pośrednictwem blockchaina odpowiednie służby uzyskałyby dowód, że jestem w swoim domu – bez konieczności ujawnienia informacji o tym, gdzie mój dom się znajduje. Ba, nawet nie dowiedziałyby się, kim jest sprawdzana przez nie osoba. By poznać dane osobowe weryfikowanego petenta, musiałyby odwołać się do wyższej instancji administracyjnej. Taką procedurę można by było uruchomić jednak dopiero w momencie, gdy delikwent złamał przepisy o izolacji. Wówczas z rządowej bazy służby porządkowe uzyskałyby wszelkie szczegółowe dane potrzebne do interwencji.

Bardzo ciekawe są zupełnie nowe możliwości, które daje blockchain w walce z pandemią – bo opisany powyżej przykład to tylko lepszy, tańszy i bezpieczniejszy ekwiwalent funkcjonalności, która już istnieje (ale pozostawia wiele do życzenia). Otóż… moglibyśmy używać „kryptoportfela pandemicznego” do obwieszczania, dokąd się wybieramy. Byłoby to dobrowolne i całkowicie anonimowe. Osobisty portfel pandemiczny byłby naszym awatarem w systemie. Codziennie – a nawet

częściej – mógłby się zmieniać. Ważne, żeby jego zadaniem było wysyłanie lokalizacji. Po stronie platformy powstawałby rejestr historii naszych spotkań ze znanymi i nieznanymi nam osobami – ot, choćby w autobusie, na koncercie, w sklepie. W razie infekcji w przychodni zostanie odczytany awatar zarażonego. Wszyscy, którzy mieli z nim kontakt, zostaną o tym fakcie powiadomieni. Nie wiemy, kim oni są – nie znamy ich imion i nazwisk – nie wiemy też, gdzie znajdują się teraz. Najważniejsze jest jednak to, że może do nich dotrzeć informacja o kontakcie z zarażonym człowiekiem. Jak to teraz wykorzystać?

Można by po prostu odwołać się do ich postawy obywatelskiej i zasugerować, by na stosowny czas ograniczyli kontakty. Można też ich zachęcić, by się przetestowali. Jeśli zareagują pozytywnie – pamiętajmy, że wszystko to odbywa się anonimowo – otrzymają stosowne poświadczenie (o izolacji lub przetestowaniu się). Takie poświadczenie mogłoby automatycznie generować rabaty przy wykupie polisy ubezpieczeniowej lub zapewniać ulgę podatkową. Państwo i tak byłoby na plusie, bo ograniczałoby w ten sposób rozprzestrzenianie się kosztownej pandemii. Zyskaliby również obywatele – test mógłby być darmowy, jeśli wykonaliby go na przykład w dwanaście godzin od otrzymania powiadomienia; zresztą już samo odwołanie wizyty u starszych rodziców byłoby z punktu widzenia zapewnienia bezpieczeństwa zdrowotnego niezaprzeczalną korzyścią.

Przyszłość już tu jest

W tym rozdziale być może nie dowiedziałeś się niczego zaskakującego, szczególnie że rozpocząłeś jego lekturę, dobrze znając zalety blockchaina i rozumiejąc, jak działa. Wyłania się jednak z niego bardzo ważna kwestia:

jak bardzo obieg danych może ułatwić wszystkim życie i przenieść jego komfort na zupełnie nowy poziom. Mimo tej oczywistej konstatacji komunikacja – szczególnie w dziedzinie opieki zdrowotnej – wyraźnie kuleje. Systemy zapewniające nieskrępowaną, a jednocześnie anonimową wymianę i analizę danych są po prostu bardzo trudne do stworzenia od zera.

Tyle że wcale nie musimy ich tworzyć! Mamy przecież gotowe rozwiązanie: blockchain, zrodzony w sieci, z jego filozofią prywatności i niezależności, który już na wejściu oferuje nam wiele narzędzi – właśnie tych, których potrzebujemy.

13

Nieruchomości

Jan wyszedł z metra i udał się w kierunku biurowca. Przyłożył zegarek do terminala przy drzwiach. Urządzenie rozbłysło czerwoną poświatą i wyświetliło smutną emotkę, a zegarek złowrogo zawibrował. No nie, tylko nie dziś… Jan otworzył aplikację portfela i dokupił tokenów biura – teraz terminal uśmiechnął się podświetloną na zielono emotką.

Jan jest dziś trochę roztargniony i podminowany, bo rano otrzymał wiadomość, że mieszkanie jego babci jest przygotowane do sprzedaży. To dla niego bardzo dziwne, jest przekonany, że babcia nie ma z tym nic wspólnego. Najprawdopodobniej padła ofiarą jakiegoś przekrętu – ma już swoje lata… „Dobrze, że użyliśmy wielopodpisowego portfela, przenosząc akt własności na nową platformę", pomyślał Jan. „Transakcja bez podpisów brata i mojego własnego nie dojdzie do skutku, ale i tak muszę skontaktować się z babcią. Pojadę do niej po pracy". Jan usadowił się za biurkiem w przestronnym gabinecie. „Świetnie mi się tu pracuje, aż żal, że ten projekt skończy się za miesiąc… Mam nadzieję, że kolejny gabinet będzie na podobnym poziomie".

Blockchain jako cyfrowa księga wieczysta

Nieruchomości to jeden z najważniejszych sektorów światowej gospodarki – budownictwo często uważane jest za wyznacznik kondycji ekonomicznej kraju. Analizując dynamikę inwestycji w tej branży, wnioskujemy, czy cała gospodarka ma się dobrze, czy dostaje zadyszki. Nieruchomości są ważne również dla nas – indywidualnych konsumentów. Zakup nieruchomości to bardzo często największy wydatek w naszym życiu, który w dodatku przesądza na lata o jego jakości.

Czy taki kolos może jeszcze podlegać jakimś zmianom?

Mieliśmy już okazję przyjrzeć się, jak publikowanie i zarządzanie aktami notarialnymi w kryptowalutowych blockchainach może wydatnie przyczynić się do usprawnienia procedur związanych z przeniesieniem własności i zabezpieczaniem interesów wszystkich stron.

Gdybyśmy dysponowali takimi mechanizmami lata temu, zapobieglibyśmy wielu nadużyciom. Myślę tu o aferach związanych z najwyższymi kręgami administracji – chodzi o nielegalne przejęcia mieszkań i kamienic.

To jednak nie wszystko. Ustandaryzowane i niepodważalnie udokumentowane w blockchainie przepływy finansów i zmiany statusu własności nieruchomości idealnie nadają się do analizy rynku. Wycena nieruchomości staje się o wiele prostsza w interpretacji w porównaniu z sytuacją, gdy transakcja jest wieloetapowym procesem. Jeśli umożliwią to zasady blockchaina i obowiązujące prawo, analizie może też podlegać struktura właścicielska. Takie badania pozwalają na przykład wykryć, jak duża część rynku znajduje się w posiadaniu firm i skąd pochodzą inwestorzy – czy są krajowi, czy zagraniczni. Uwagę regulatora mogą w szczególności wzbudzić nieruchomości należące do firm zarejestrowanych w rajach podatkowych.

Jeśli do obsługi „nieruchomościowego” blockchaina – cyfrowego odpowiednika ksiąg wieczystych – będzie prawnie wymagane używanie państwowego dokumentu identyfikacyjnego (pod postacią stosownego klucza kryptograficznego), znikną wszelkie możliwości ukrywania funduszy w nieruchomościach, czyli prania pieniędzy. Takie próby zostaną od razu wykryte przez urząd skarbowy, również dysponujący kryptograficznym kluczem dostępu.

Mamy więc pełną transparentność. Co dobrego z niej jeszcze wynika?

Zarządzanie prawami własności na jednej platformie sprawia, że łatwo otworzyć ją na cały świat, co może katalizować zagraniczne inwestycje. Jasne zasady kupna i sprzedaży – z jednej strony zakorzenione w prawie, a z drugiej wyrażone smartkontraktami i strzeżone kluczami kryptograficznymi – mogą w przyszłości być lepiej widziane niż papierowa kopia aktu notarialnego w kancelarii w jakimś kraju na drugim końcu świata.

Stop przekrętom, czas na rozwój

A co powiesz na taki oto zupełnie nowy efekt digitalizacji procesu zarządzania nieruchomościami? Otóż obywatele mogą wydatnie pomagać państwu w planach zagospodarowania przestrzennego. Jeśli zarządzający nieruchomościami blockchain nadbudujemy warstwą mapy z przyjętym planem miasta czy gminy, w zasadzie zniknie pole do nadużyć. Na pewno pamiętasz, że bloki z transakcjami w blockchainie zawierają kompletną historię wszystkich zmian. Jeśli więc dojdzie do jakiejkolwiek nieuprawnionej zmiany i w nieoczekiwanym miejscu pojawią się plany budowy fabryki czy biurowca, niezadowoleni mieszkańcy tego terenu

szybko udowodnią swoje racje organom wydającym pozwolenie na budowę. Mogą odwołać się do historycznego bloku, w którym zagwarantowano mieszkaniowy charakter parceli. Mogą nawet dociec, który urzędnik wprowadził zmiany w planach. W standardowych systemach, w których wszystkie dane da się nadpisać, byłoby to niezwykle trudnym zadaniem: autorzy zmian nie są w nich identyfikowani przez klucze prywatne i pole do nadużyć jest znacznie większe.

Opisana historia mogłaby się potoczyć zupełnie innym torem. Zakładając, że ustawodawca dopuści taką możliwość, inwestor mógłby zaaplikować w blockchainie o zmianę charakteru gruntu tak, by odpowiadał planowanej przez niego inwestycji. Blockchain, który zapewnia anonimowość wszystkim stronom, pozwoliłby – w odpowiedzi na zapytanie inwestora – przeprowadzić głosowanie sąsiadów, a nawet całej dzielnicy czy gminy. Mogłoby się okazać, że nowa inwestycja jest przez nich pożądana i zdecydowanie polepszy ich standard życia. A gdy zostanie ukończona, blockchain pomoże rozdysponować odpowiednim organom roszczenia tych spośród sąsiadów inwestycji, którzy w jakiś sposób zostali nią dotknięci. Zamiast korupcji (lub stagnacji) – rozwój!

Dzielenie włosa na czworo, a biurowca na milion

Sztandarowym przykładem wpływu technologii kryptowalut na nieruchomości jest tak zwana tokenizacja. Zetknęliśmy się już z tym zagadnieniem przy okazji opisu działania serwisu streamingowego w blockchainie. Pojawiła się tam technologia smartkontraktów, czyli interaktywnych cyfrowych umów. W przypadku serwisu filmowego umowa (smartkontrakt) przypominała co do zasady umowę spółki akcyjnej.

Zamiast akcji otrzymywaliśmy jednak monety nowej waluty (tokeny). Dzięki nim mogliśmy korzystać z serwisu. Właściciel smartkontraktu mógł w ten sposób pozyskać fundusze do finansowania rozwoju firmy. Jest to tradycyjny model znany z klasycznej giełdy papierów wartościowych – koła zamachowego każdej rozwiniętej gospodarki.

Tokenizacja jest czymś analogicznym. Zresztą często używa się jej do realizacji smartkontraktów. Różnica polega na tym, że w przypadku tokenizacji realizowany za jej pomocą smartkontrakt zwykle zawiera fizycznie istniejące aktywa lub coś trwałego i wartościowego – na przykład mieszkanie, biurowiec, parcelę, ale także… klasyczny, zabytkowy samochód. Gdy podzielimy przedmiot smartkontraktu na małe cząsteczki, stanie się on czymś na wzór spółki akcyjnej. Te cząsteczki – wyrażone kryptowalutowymi monetami – to właśnie tokeny. Ich sumaryczna wartość w naszym portfelu odpowiada naszemu procentowemu udziałowi w danych aktywach. Nie ma tu żadnych ograniczeń związanych z „dzieleniem" aktywu na tokeny: wspomniany samochód możemy „podzielić" na dziesięć lub sto tokenów, ale olbrzymi biurowiec o zawrotnej wartości pewnie będzie lepiej „podzielić" – czyli stokenizować – na milion lub nawet więcej tokenów.

Czy te tokeny przypadkiem z czymś ci się nie kojarzą? Tokeny – części czegoś wartościowego, z przypisanym do nich prawem własności, niepodważalnie udokumentowanym w blockchainie? Tak, to oczywiście NFT! Tu jednak NFT występuje w niezwykle dojrzałej, poważnej odmianie, bardzo dalekiej od medialnie utrwalonego skojarzenia, że „NFT to jakieś głupie obrazki z internetu".

Jakie są konsekwencje tokenizacji nieruchomości?

Przede wszystkim płynność. Nieruchomości są fundamentalną częścią wielu strategii inwestycyjnych. Dla przeciętnego człowieka mają jednak

bardzo wysoki próg wejścia. Statystyczny Kowalski zarabia za mało, by móc zainwestować w jakąś intratną nieruchomość, której wartość może jeszcze wzrosnąć z czasem. Oczywiście przychodzą tu na pomoc fundusze inwestycyjne – REIT-y (*Real Estate Investment Trust*); oprócz wielu zalet, mają jednak wady. Podstawową wadą REIT-ów jest to, że są produktem finansowym obejmującym większą grupę nieruchomości. Tokenizacja za to doskonale sprawdza się w podziale konkretnego elementu aktywów: apartamentowca, biurowca, mieszkania czy… klasycznego oldtimera.

Po stokenizowaniu nieruchomości kolejny krok to giełda – tam tokeny aktywów stają się dostępne dla szerokiego grona odbiorców. Jest to rynek bardzo płynny i dynamiczny, szczególnie jeśli porównać go do nieco ociężałego tradycyjnego rynku nieruchomości, gdzie w większości wypadków przedmiotem handlu są całe mieszkania, domy, działki – a nie ich części.

Do czego (jeszcze) mogą się przydać tokeny

Tokeny nie tylko rewolucjonizują posiadanie nieruchomości. Mogą mieć bardzo użytkowy charakter. Nasz bohater z historyjki otwierającej rozdział nie wykupił tokenów biura, a system inteligentnej automatyki biurowca działa w połączeniu ze smartkontraktem obsługującym płatności. Smartkontrakt nie odnotował wpłaty i usunął klucz Jana z listy uprawnionych do wejścia. To bardzo wszechstronny mechanizm. Administrator biurowca przed udzieleniem dostępu do wnętrza budynku może zażądać od nas więcej danych – i to bez podawania tożsamości. W sposób w pełni zautomatyzowany możemy choćby udowodnić brak zadłużenia, niekaralność, zerowy bilans w rozliczeniach z fiskusem i tym

podobne. Dzięki blockchainowi cały ten proces jest przeprowadzany anonimowo i automatycznie. My zachowujemy prywatność, a administrator nieruchomości otrzymuje niepodważalne dowody prawdziwości wymaganych przez niego danych.

W tym miejscu krótka dygresja pod postacią garści oficjalnej terminologii. W świecie blockchaina procedury identyfikacji klienta określa się dwoma skrótami: KYC (*Know Your Customer*, czyli dosłownie „znaj swojego klienta") oraz AML (*Anti-Money Laundering Policy*, „polityka przeciwdziałania praniu pieniędzy"). KYC i AML są stosowane głównie przez instytucje finansowe – na przykład giełdy, dla których stanowią niemal obowiązkową procedurę, w szczególności wobec kont dokonujących większych transferów.

Wróćmy do przykładu pracy w biurze: Jan mógłby kupić część biura zamiast dostęp do biura. Zasady, takie jak ta, która mówi, ile tokenów uprawnia do korzystania z biura, również określa się w smartkontrakcie. System biur częściowych lub chwilowych staje się coraz bardziej popularny – wynika to ze stylu pracy freelancerów, niepotrzebujących ani całego obiektu biurowego, ani biura na dłuższy czas. Również zbycie stanowiska biurowego po zakończeniu projektu, do którego było potrzebne, w świecie kryptowalut staje się trywialne.

Tokenizacja daje wszystkim wielką swobodę w określaniu praw i obowiązków właścicieli tokenów reprezentujących nieruchomość. W naszym przykładzie tokeny mogą odzwierciedlać wszelkie aspekty ekosystemu biurowca i być podzielone na rozmaite kategorie: tokeny stanowisk biurowych, tokeny parkingowe, tokeny usług spożywczych, a być może już niedługo tokeny dróg powietrznych dla dronów dostarczających przesyłki. Możliwości tkwiące w warstwie właściwości tokenów są praktycznie nieograniczone. Z jednej strony usprawnia ona

transfery na rynku nieruchomości, z drugiej – zarządzanie i korzystanie z budynku.

To nie wszystko. Płynność i dynamika blockchaina optymalizuje kwestię opłat i wynagrodzenia. Właściciel biura ponosi koszty administrowania budynkiem, ale zarabia na jego zautomatyzowanym wynajmie. Co więcej, dzięki dostępniej w blockchainie publicznej księdze rachunkowej łatwo sprawdzi, czy zarządca budynku rzetelnie realizuje swoje zadania.

Out of office, czas na timeshare

Z codziennej biurowej orki przenieśmy się… na wakacje! Na najpiękniejszych wybrzeżach naszej planety często powstają luksusowe hotele i apartamentowce. Mało popularnym w Polsce, a w innych krajach dość znanym sposobem wykupu nieruchomości wczasowych jest tak zwany system timeshare, czyli dosłownie „współdzielenie czasu”. Polega on na wykupie dostępu do nieruchomości (na przykład apartamentu) na określony czas (zwykle na dwa lub trzy tygodnie w roku). Tym sposobem 52 tygodnie roku – przy systemie dwutygodniowym – są rozdzielone między 26 właścicieli. I tak oto nieruchomości, które w atrakcyjnych lokalizacjach są znacząco droższe niż gdzie indziej, stają się dostępne za cząstkę swojej ceny. Rynek timeshare, jak łatwo sobie wyobrazić, jest bardzo dobrze rozwinięty.

Jak mogłyby wspomóc go tokeny? Na dwa sposoby. Pierwszy z nich: system tokenów kryptowalutowych mógłby być wykorzystany przez firmy administrujące i sprzedające nieruchomości. Uprościłoby to rozliczenia i zautomatyzowało komunikację. Drugi: dodatkowe korzyści klientów,

którzy przestaliby być „uwiązani” na resztę życia z jedną wakacyjną nieruchomością. Dzięki giełdom tokenów mogliby je swobodnie wymieniać na inne lub choćby wypożyczać, kiedy na przykład nie mogą skorzystać ze swojego przydziału czasu. A nad wszystkim tym czuwałaby kryptografia i blockchain.

Dla przeciętnego człowieka

Nieruchomości. Jeden z najważniejszych aspektów naszego życia. Są drogie, ale warunkują byt i rozwój; jednocześnie stanowią bezpieczną inwestycję, choć dla wielu wciąż nieosiągalną. Tradycyjny rynek nieruchomości sprawia wrażenie mało dynamicznego – jest skostniały, powolny, czasochłonny. Blockchain odświeża go powiewem innowacji. W wyjątkowy sposób łączy świat wirtualny z rzeczywistym. I najlepsze jest to, że beneficjentami tego odświeżenia będą przede wszystkim zwykli ludzie o przeciętnych dochodach, bo nagle okaże się, że będzie ich stać na zabezpieczenie swoich oszczędności inwestycją w nieruchomości.

Zmieni się również nasze życie codzienne. Zauważ, jak pandemia zmieniła nasz stosunek do wykonywania pracy: staliśmy się dynamiczni, polubiliśmy się z pracą zdalną, jesteśmy otwarci na częste zmiany. Ta przemiana dokonała się co prawda wbrew naszej woli, ale ogólnie rzecz biorąc, ma całkiem pozytywny charakter. Podobnie będzie z kryptowalutami, które zdynamizują rynek nieruchomości, zwiększając jego płynność. Takie zmiany świetnie się wpisują w wymagania klientów biur i hoteli, dla których liczy się maksymalna elastyczność i szybkość reakcji. Dzięki kryptografii i nienaruszalności zapisów w księdze rachunkowej blockchaina kurczy się do minimum pole do nadużyć, prania

brudnych pieniędzy i korupcji. A mechanizm tokenizacji możemy wykorzystać nie tylko do inwestowania w nieruchomości, ale także w ruchome dobra: w klasyczny samochód, rzeźbę lub obraz. I nawet gdyby miała to być niewielka rodzinna inwestycja, zbyt mała, by opłacało się powoływać spółkę, zawarcie umowy opisanej smartkontraktem operującym na tokenach zapewni wszystkim jej stronom spokojny sen.

14

Demokracja

Dwa aspekty państwowości

Czym jest dla mnie państwo?

Postrzegam je w dwóch kategoriach.

Pierwsza to cały państwowy aparat administracyjny, który reguluje, a przez to kreuje otaczającą nas rzeczywistość.

Sądy, księgi wieczyste, komunikacja, policja, wojsko, system ochrony zdrowia, edukacja, finanse i tak dalej – słowem: instytucje państwowe i cały administracyjny krwiobieg, który je zasila, łączy oraz sprawia, że tak rozległa organizacja funkcjonuje i zapewnia obywatelom przestrzeń do działania.

Wiele z tych zagadnień już poruszyłem, omawiając zmiany, jakie może w do naszego życia wprowadzić blockchain. Przypomnę tylko, że dzięki niemu zyskujemy na korzystaniu z sieciowych protokołów, które nie tylko standaryzują i ułatwiają komunikację, ale – co równie istotne – szanują naszą prywatność i własność. Ponadto zyskujemy automatycznie zdolność audytu funkcjonowania aparatu państwowego.

Jeden z aspektów tego aparatu, który budzi we mnie oburzenie, to domyślna niejawność transakcji w państwowej sferze budżetowej. Dlaczego każda faktura każdego ministerstwa nie trafia do otwartej bazy danych? Przecież to nasze wspólne pieniądze i nasze wspólne państwo. Teoretycznie można się ubiegać o ujawnienie szczegółów państwowych wydatków, ale proces pozyskiwania tych informacji pozostawia wiele do życzenia i jest skutecznie zniechęcający. Kwerendy i zapytania, które są zbywane jednym podpisem czy wieloetapowe dochodzenie do prawdy przez organizacje społeczne i pozarządowe – to nie buduje zaufania do struktur państwowych.

Dlatego uważam, że migracja administracji państwowej do blockchaina byłaby bardzo pożądana – w ten sposób obywatele zyskaliby pełną transparentność działania instytucji opłacanych z ich podatków. Dzięki temu, że blockchain jest publiczną, audytowalną i nienaruszalną bazą danych, wszystkie operacje przez lata byłyby jawne dla entuzjastów patrzenia władzom na ręce, społeczników, a także działających w blockchainie programów, które wykrywają podejrzane transfery. Myślę, że już sama wizja niemożności ukrycia przestępstw i nadużyć w sferze państwowej odniosłaby należyty skutek – zniechęcałaby do tego, co sprawia, że polityka jest aktualnie uważana za „brudną”. To mógłby być fundament silnych i profesjonalnych struktur państwowych. Wyniki wyborów, niezależnie od tego, która opcja wygra, nie mogłyby zakłócić prawidłowego działania tych struktur. Blockchain wyznaczyłby w końcu tak potrzebną nam wszystkim granicę oddzielającą służbę cywilną od polityki.

Druga zasadnicza kategoria spraw państwowych to właśnie wybory: parlamentarne, prezydenckie, samorządowe oraz wszelkie referenda.

Żyjemy w demokratycznym kraju i korzystamy z prawa do wolnych, anonimowych wyborów.

Ostatnimi czasy w niektórych demokratycznych krajach pojawiły się symptomy kryzysu demokracji i kontrowersje wokół wyborów. Nie mam na myśli wyłącznie młodych demokracji, takich jak Polska, gdzie partia rządząca kwestionowała niepomyślne dla niej wyniki wyborów samorządowych, a później na bardzo wątpliwych pod względem wiarygodności zasadach usiłowała przeprowadzić wybory kopertowe. Również w kolebce nowożytnych demokracji – Stanach Zjednoczonych – doszło do poważnego kryzysu. Ustępujący prezydent Donald Trump nie chciał uznać wyników wyborów, oskarżył demokratów o manipulacje przy liczeniu głosów i chęć odebrania mu jego rzekomego zwycięstwa oraz zachęcił zgromadzony przed Białym Domem tłum do szturmu na Kapitol. Sytuację opanowano (nie obyło się bez ofiar śmiertelnych i rannych, głównie wśród policjantów), a władzę zgodnie z prawem przejął Joe Biden.

Dlaczego wyniki wyborów miałyby wzbudzać jakiekolwiek wątpliwości? Co może wywoływać dyskusje i spory dotyczące manipulacji i nadużyć podczas demokratycznych plebiscytów? Odpowiedź jest prosta: liczenie głosów, przewożenie urn wyborczych, wybory korespondencyjne, głosowanie w instytucjach zamkniętych, głosowanie za nieświadome w pełni osoby – wszystkie te aspekty mogą stawiać pod znakiem zapytania wiarygodność części oddanych głosów. A wszystko przez to, że głosujemy na anonimowej kartce.

Głosowanie przez internet

Czy istnieje technologia, która zapewnia nie tylko anonimowość, ale i możliwość weryfikacji oddanego głosu? Tak! To oczywiście blockchain.

Kiedy zastanawiam się, jak powinno przebiegać nowoczesne głosowanie, mam taką wizję:

W dniu wyborów oddaję głos w aplikacji na swoim smartfonie. Głos ten przesłany jest do komisji wyborczej, czyli węzła blockchaina. Smartkontrakt po zamknięciu wirtualnych urn zlicza głosy. System kryptograficznie zabezpieczonych kont i podpisów zapewnia, że głosy pozostają tajne do zakończenia głosowania. Następnie komisja wyborcza podaje do wiadomości wynik plebiscytu. Najważniejszy etap – z punktu widzenia weryfikacji głosu – to właśnie ten moment po opublikowaniu wyników. Każdy głosujący może sprawdzić, czy jego głos został policzony, a jeśli tak, to czy znalazł się przy tym nazwisku, na które rzeczywiście głosował. Dzięki procedurom kryptograficznym odbędzie się to z zachowaniem anonimowości.

To chyba największa różnica w stosunku do tego, jak przebiegają wybory obecnie: będziemy mogli przeprowadzić samodzielnie audyt naszego głosu! Wyniki przestaną być podważane w jakikolwiek sposób. Niezadowolona strona będzie mogła co najwyżej wezwać swoich zwolenników do masowego sprawdzenia głosów. Gdyby została oszukana, bez problemu znajdzie dowody. Jeśli zaś wszystkie głosy zostały prawidłowo przypisane i zliczone, zobaczy, że… po prostu faktycznie przegrała.

Myślę, że przeprowadzanie wiarygodnych elektronicznych wyborów może być brane pod uwagę jedynie w zdecentralizowanym systemie. Tymczasem – paradoksalnie – jest ono wdrażane w formie scentralizowanej, gdyż tak jest taniej i wygodniej. Klasyczne centralne systemy kryją w sobie zbyt wiele niejawnych procesów, by zaufać im

w pełni. Narażają naszą anonimowość i poufność naszych wyborów – „wiedzą”, na kogo głosowaliśmy, zatem znają naszą orientację polityczną. Za weryfikację głosowania odpowiada centralny strażnik – to, co powie, jest święte i ostateczne, a my w żaden sposób nie możemy tego sprawdzić. Elektroniczne wybory w systemie scentralizowanym to praktycznie ten sam arbitralny i zamknięty proces jak przy liczeniu klasycznych kart do głosowania – tak samo wzbudza wątpliwości i nieufność.

W tym miejscu chcę jednak oddać sprawiedliwość krytykom blockchaina jako technologii obsługującej głosowanie. Istnieje bowiem ciekawy artykuł ekspertów od cyberbezpieczeństwa, zatytułowany „Ze złego na gorsze: od głosowania internetowego do głosowania w blockchainie”*. Autorzy przeprowadzili w nim szczegółową i dogłębną analizę możliwych ataków na blockchainowy system głosowania. Nie będę wchodził w detale, ale nawet tak powszechne zagrożenia jak exploity zero-day, podsłuchiwanie czy odmowa dostępu DDOS na pewno znajdą się w inwentarzu podmiotów, które chcą wpłynąć na wynik wyborów. Taki wpływ zawsze stanowi łakomy kąsek chociażby dla służb wrogich krajów. Podsumowując, autorzy wspomnianego artykułu rekomendują użycie blockchaina jedynie jako równoległego narzędzia sondażowego, a z uwagi na koszt ataku w stosunku do możliwości wpłynięcia na wynik wyborów, zalecają odejście od wszelkich elektronicznych metod oddawania głosów oraz powrót do klasycznych, papierowych kart. Tylko one – zdaniem autorów – przez swój fizyczny charakter ograniczają realny wpływ ewentualnych fałszerstw.

Rozumiem to doskonale i może nawet bardziej niż inni zdaję sobie sprawę z wszelkich zagrożeń. Patrzę jednak na to zagadnienie z nieco innego punktu widzenia: z jednej strony scentralizowane systemy do elektronicznego głosowania są już powoli wdrażane, z drugiej – mamy

silnie spolaryzowane społeczeństwa podatne na manipulacje, co też przecież nadweręża stabilność ustrojów. Jeżeli zatem nie ma odwrotu od głosowania przez internet, przeprowadzajmy je porządnie i najbezpieczniej, jak się da – czyli w blockchainie.

Płynna demokracja

Zauważmy, że znów rozmawiamy o technikaliach. Papier, impuls elektromagnetyczny, błysk w światłowodzie – to tylko technologie. Czy blockchain może zmienić proces demokratyczny w jakiś głębszy sposób?

Jednym z szeroko dyskutowanych pomysłów, i to już od co najmniej stu lat, jest płynna demokracja (*liquid democracy*) – coś pomiędzy demokracją bezpośrednią a republiką.

Przypomnijmy, że republika to ustrój, w którym wybieramy swoich przedstawicieli. W naszym imieniu sprawują oni władzę ustawodawczą i wykonawczą. Demokracja bezpośrednia jest natomiast ustrojem, w którym obywatel ma możliwość głosowania nad każdym aktem państwowym.

To chyba oczywiste, na czym polega problem z demokracją bezpośrednią… Raczej nie spotkamy się na stadionie mieszczącym 40 milionów osób (nie tylko dlatego, że PGE Narodowy zapewnia tylko 72 tysiące miejsc), by kulturalnie debatować nad wszystkimi możliwymi ustawami. Republika również nie jest idealnym ustrojem. Posłowie po otrzymaniu mandatu zapominają o wyborczych obietnicach, a dyscyplina klubowa to dla nich krępujące indywidualną inicjatywę jarzmo, często zresztą zmuszające ich do głosowań wbrew osobistym przekonaniom.

Płynna demokracja jest sposobem na delegowanie swojego głosu wybranemu parlamentarzyście. On zaś może oddać swój głos i wszystkie inne, które do niego spłynęły. Swojego głosu możemy użyczyć na określony czas, oddać go na określoną ustawę lub tylko w określonej dziedzinie. No i w każdej chwili nasz głos możemy wycofać. W ideę płynnej demokracji wpisana jest grawitacja prawa do głosowania, działająca w kierunku ekspertów z danej dziedziny. Naturalną konsekwencją takiego postawienia sprawy jest stworzenie rodzaju merytokracji, czyli tego, na czym wszystkim zależy i co szumnie obiecują wszystkie partie (gorzej z realizacją tych obietnic). Chodzi mianowicie o rząd ekspertów.

Z technicznego punktu widzenia mamy już wszystko, by można było wprowadzić demokrację bezpośrednią. Mimo pewnych – bardziej teoretycznych niż praktycznych – zalet takiego rozwiązania, ustrój ten wcale nie musi jednak się sprawdzić. Powód jest prosty: brak szerokiej wiedzy – ogólnej, eksperckiej i dotyczącej zarządzania państwem – u (niestety) przeważającej części obywateli. Z tego też wprost wynika podatność omawianego ustroju na manipulacje i populizm. Ale paradoksalnie największym jego problemem mogłoby się okazać coś innego: niechęć większości do angażowania się w sprawy społeczne. Demokracja bezpośrednia mogłaby wówczas zostać przejęta przez mniejszość obywateli. Tego problemu doświadczamy zresztą już dziś – wystarczy przywołać frekwencję wyborczą z ostatnich lat.

Płynna demokracja jest pośrednią formą rządzenia państwem. To coś pomiędzy posiadaniem reprezentanta, na którego oddaliśmy głos w wyborach, a oddawaniem głosu zgodnie ze swoim upodobaniem.

Zauważmy, że w przypadku płynnej demokracji blockchain daje nam narzędzia do walki z wszelkimi nadużyciami. Szczególnie jeśli chodzi

o wrażliwe kwestie etyczne, gdzie tak ważna jest anonimowość – moglibyśmy z jej pełnym dochowaniem weryfikować, czy nasz przedstawiciel rzeczywiście zagłosował w pożądany sposób.

Płynna demokracja jest ciekawym sposobem zbalansowania wpływów pełnoetatowych polityków i zwykłego, ale zaangażowanego obywatela, który prawa uchwalanego przez swoich reprezentantów doświadcza na własnej skórze.

Pamiętajmy, że płynna demokracja jest zupełnie dobrowolna. Jeśli nie będzie nas interesowało śledzenie legislacji, po prostu wydelegujemy nasz głos na dowolny czas znanemu z telewizji lub plakatu politykowi, który wzbudza nasze zaufanie i pod którego decyzjami chcemy się podpisywać. Gdy polityk zmieni poglądy lub w inny sposób zawiedzie nasze zaufanie, głos przekażemy komuś innemu. To świetny pomysł na dyscyplinowanie polityków, którzy upojeni władzą zapominają, że są naszymi reprezentantami i muszą postępować tak, jak sobie tego życzymy.

Liberalny radykalizm

Dlaczego spór o politykę zawsze budzi tyle kontrowersji? Dlaczego politycy mają tak wielki wpływ na nasze życie? Myślę, że jedną z tych bardziej oczywistych przyczyn jest rozporządzanie budżetem. Żyjemy w zróżnicowanym społeczeństwie. Mamy różne cele. Oczekujemy od władzy zróżnicowanych działań. Jak je pogodzić? Jak sprawiedliwie rozdysponować zgromadzone w budżecie środki?

Vitalik Buterin, twórca kryptowaluty ethereum, wraz z naukowcami zajmującymi się ekonomią, Zoë Hitzig oraz Glenem Weylem, w swoim

artykule przedstawili mechanizm neutralnego odkrycia wspólnych celów społecznych**.

„Liberalny radykalizm: elastyczny sposób przydziału środków wsparcia” to moja najlepsza próba przetłumaczenia tytułu tej pracy. Niestety nie oddaje ona wieloznaczności słów, wskazującej na pochodzenie opisanej w niej metody. *Radical* w języku angielskim może odnosić się również do symbolu pierwiastkowania liczby. Gdy poznamy formułę rozdziału dóbr, ta aluzja stanie się oczywista.

Celem badań opisanych w powyższej pracy był projekt takiego rozdysponowania wspólnego budżetu, by promował wspólne potrzeby. Projekt ów jest – jak podkreślono w tytule – bardzo elastyczny i przedstawia pewien uniwersalny zamysł. W szczególności dotyczy sytuacji, w której wspólny budżet wspierałby oddolne inicjatywy. Oto wypracowana przez autorów formuła podziału:

Wsparcie finansowe projektu jest proporcjonalne do kwadratu sumy pierwiastków przeznaczanych na nią składek.

I od razu przykład, żebyś dobrze zrozumiał, na czym ta formuła polega.

Załóżmy, że składki wpłacane na konto organizacji realizującej różne projekty mogą być wpłacane bezpośrednio. Formuła mówi, na co wydać jej środki i w jakiej proporcji. Te składki możemy interpretować jako podatki celowe i wtedy całość rozważań odniesie się do budżetu publicznego.

Zatem: jeśli pięć osób zdecyduje się wskazać pewną inicjatywę, czyli jakiś projekt, poprzez przekazanie na nią 100 złotych z zapłaconych przez

siebie podatków, wówczas zgodnie z formułą budżet wesprze tę inicjatywę kwotą (10 to pierwiastek ze 100, a tyle wynosi składka):

$$(10+10+10+10+10)^2 = 50^2 = 2500 \text{ zł}$$

Jeśli jakaś inna inicjatywa będzie miała tylko jednego wspierającego, ale za to takiego, który przeznaczy na nią aż tysiąc złotych, to i tak otrzyma ona dodatkowe wsparcie ze wspólnego budżetu, ale w wysokości… tylko tysiąca złotych (pierwiastkujemy i podnosimy do kwadratu – czyli otrzymujemy to samo).

Zauważ, że ponieważ w pierwszym przypadku jakiś cel przyciągnął aż pięciu podatników, to mimo mniejszych składek formuła „uznała” go za ważniejszy! Czyli bardziej od wysokości składek premiowana jest jednomyślność.

Autorzy cytowanej pracy utrzymują, że odnaleźli metodę na najefektywniejszy rozdział środków przy jednoczesnym zminimalizowaniu potencjalnych konfliktów.

Podam tu za autorami bardzo ciekawy przykład z życia codziennego. Dobrym zastosowaniem metody radykalnego liberalizmu jest wybór państwowej agencji informacyjnej – lub telewizji – która będzie finansowana z naszych podatków. Myślę, że w Polsce każdy właściciel telewizora wie, że u nas to duży problem.

Zgodnie z omawianą formułą najwięcej środków powinna otrzymać ta agencja, która będzie wspierana przez największą grupę odbiorców. Ale to nie wszystko! Jak ta formuła zabezpieczy obiektywność wybranego medium? Przecież na pierwszy rzut oka nie widać w niej tego mechanizmu. Bez obaw! Przekazywanie obiektywnych i pełnych informacji będzie się opłacać, bo populistyczne i propagandowe przedstawianie wydarzeń na

pewno spolaryzuje widownię. I jeśli od stacji/kanału/agencji odwróci się połowa widzów, strata wcale nie wyniesie tylko połowy finansowania. Fundusze zmniejszą się aż o trzy czwarte! Zostanie jedynie ćwierć pierwotnej sumy.

Smartkontrakt w blockchainie jest idealnym narzędziem do realizacji takich sztywnych reguł dystrybucji środków. Odbiera politykom uznaniowość w dysponowaniu naszymi pieniędzmi. Walczy z korupcją i umieszczaniem krewnych i znajomych wygranej partii w spółkach skarbu państwa.

Prawdopodobnie autorzy pracy o radykalnym liberalizmie również zdawali sobie sprawę, jak wielkim wyzwaniem jest ta idea… Stąd słowo „radykalny” w pierwotnym (a nie pierwiastkowym) znaczeniu w nazwie metody rozdziału środków. Koncepcja przedstawiona w artykule jest odpowiedzią na narastający kryzys zaufania do władz. Liberalny radykalizm to ruch postpolityczny.

Dotychczasowe sposoby łagodzenia konfliktów zbyt głęboko ingerują w politykę monetarną, grożąc stagnacją, monopolami i deterioracją demokracji w państwie. Jak zauważają autorzy pracy, libertariańskie modele nie sprawdziły się, a lokalne społeczności, które powinny być naturalnym katalizatorem porozumienia, zostały zdominowane przez rozproszone grupy w sieciach społecznościowych. Przyszłość będzie cyfrowa, a liberalny radykalizm to rozwiązanie, które idealnie się w niej sprawdzi.

Quadratic Voting – głosowanie kwadratowe

Metoda radykalnego liberalizmu stanowi rozszerzenie innej bardzo ciekawej koncepcji, która być może w przyszłości wpłynie na sposób liczenia głosów.

Na przykładzie finansowania telewizji publicznej przekonaliśmy się, jak dobrze działa zwykła, prosta i zawsze obiektywna matematyka. Utrata połowy widzów wywołuje aż czterokrotną – a nie dwukrotną! – utratę środków.

Mechanizmem o podobnej sile oddziaływania jest głosowanie kwadratowe. W tej metodzie każdy uprawniony do głosowania obywatel otrzymuje więcej niż jeden głos. Na przykład dziesięć. Takie rozwiązanie świetnie się sprawdza w przypadku referendów z kilkoma niewykluczającymi się opcjami – zliczane są kwadraty wartości oddanych przez nas głosów.

Oto przykład: mamy referendum, a w nim do rozstrzygnięcia dziesięć spraw (oznaczonych literami od A do J). Każdy obywatel otrzymuje do rozdysponowania dziesięć głosów. Jeśli zagłosuje za każdą sprawą, jego głos przy każdej z nich będzie miał jednakową siłę: jeden. Jeśli natomiast zechce pokazać, że szczególnie ważnych jest dla niego kilka konkretnych zagadnień, może przy nich oddać więcej głosów, ale tak, by wszystkie głosy nadal sumowały się do dziesięciu. Przez to, że ma ich tylko dziesięć, będzie musiał zrezygnować z głosowania na niektóre opcje. Aby powiększyć wpływ tej często dramatycznej decyzji, głosy są zliczane po podniesieniu ich liczby do kwadratu. Zatem jeśli w sprawie A obywatel oddał pięć głosów, w sprawie B – trzy, a w sprawie C – dwa, to po przeliczeniu w sprawie A zagłosował z siłą dwudziestu pięciu głosów, w sprawie B – dziewięciu, a w sprawie C – czterech. W sprawach od D do J nie oddał głosu – były mu one obojętne albo nie tak ważne, jak sprawy od A do C, dla których zdecydował się poświęcić resztę spraw.

Uważam, że to bardzo ciekawy mechanizm. Likwiduje bowiem problem dyskryminacji mniejszości w procesach demokratycznych. Może też znaleźć zastosowanie w korporacjach przy rozmaitych ankietach.

Assurance Contracts – kontrakty koordynacyjne

Przejdźmy do lżejszych tematów. Demokracja działa nie tylko w skali państw. Udało się ją skomercjalizować!

W życiu codziennym ekonomia i psychologia nieustannie się przenikają. Podejmujemy wiele decyzji, nie zdając sobie sprawy, jakie odnoszą skutki w ujęciu globalnym. Działamy po prostu w imię własnego dobra i zwykle nie mamy okazji do refleksji nad szerszą perspektywą konsekwencji naszych wyborów.

Przykładem prób koordynowania działań większej grupy ludzi jest Kickstarter. To serwis, którego zadaniem jest zbieranie funduszy na ciekawe projekty. Znajdziemy tam wynalazców, artystów i przedsiębiorców. Oferują swoje projekty, zachwalają je inspirującymi filmami i podają, ile potrzeba im pieniędzy na realizację planów. Jeśli projekt wypali, fundatorzy stają się jego beneficjentami – zwykle jako pierwsi otrzymują zasponsorowane produkty, i to w bardzo okazyjnych cenach, na przykład za połowę ceny rynkowej.

Co więc wyróżnia Kickstarter i wiele jego klonów*** spośród innych modeli crowdfundingu, czyli zbiórek społecznościowych? Otóż fundusze są przekazywane przedsiębiorcom dopiero wówczas, kiedy osiągną zadeklarowany przez nich poziom. Jeśli projekt nie zyska odpowiedniej popularności, jego sponsorzy otrzymają zwrot środków. Daje im to

poczucie bezpieczeństwa i chroni przed ryzykiem związanym z produktowymi niewypałami i manipulacją.

To dość standardowy mechanizm, pozwól więc, że przedstawię jego ciekawe warianty.

Jednym z nich jest popularyzowany przez profesora Alexa Tabarroka kontrakt dominującej strategii koordynacyjnej (*dominant assurance contract*). Pozostańmy przy przykładzie Kickstartera, taki kontrakt zmieniłby zasady gry w następujący sposób: gdy zbiórka funduszy nie osiągnie deklarowanego przez autora projektu poziomu, nie tylko zwróci on wpłacone przez fundatorów środki, ale także wypłaci im bonus. Eksperymenty z takimi kontraktami udowodniły, że ich skuteczność w realizacji projektów jest o połowę większa niż w standardowym podejściu.

Kickstarter dobrze tłumaczy zasadę, jednak kontrakty koordynacyjne sprawdzają się świetnie przy finansowaniu inwestycji publicznych. Minimalizują one problem tak zwanego efektu gapowicza. Wyobraźmy sobie, że społeczność małego miasteczka składa się na rewitalizację parku. Park będzie cudowny, jeśli zrzucą się wszyscy… Chytry Feluś szybko dochodzi do wniosku, że będzie mógł spacerować po parku nawet bez swojego udziału w finansowaniu inicjatywy. Staje się przysłowiowym gapowiczem.

Kontrakt koordynacyjny bardzo skutecznie wspomoże stworzenie parku, gdyż burmistrz nie będzie mógł zacząć rewitalizacji, dopóki nie zgromadzi minimalnej kwoty. A efekt gapowicza zostanie zminimalizowany, bo spryt ulokuje się w chęci zarobienia na ewentualnym niepowodzeniu projektu.

Kontrakty koordynacyjne pokazują swoją prawdziwą moc w zastosowaniach pozafinansowych. Jednym z przykładów jest kontrakt

ujawniający tożsamość sygnatariuszy dopiero wówczas, gdy zbierze się ich zadeklarowana w kontrakcie liczba. Może być to ważne zabezpieczenie, które koordynuje grupę nieznających się osób – jeśli wiedzą, że ich tożsamość zostanie ujawniona dopiero po tym, jak zbierze się ich większa grupa, to nie dadzą się zastraszyć. Będą wiedziały, że nie działają w pojedynkę. Sygnatariuszami mogą być pracownicy jakiejś firmy, ujawniający naruszenie w niej zasad bezpieczeństwa. Mogą nimi być osoby upubliczniające wrażliwe sprawy przemocy seksualnej. Już samo istnienie kontraktu zachowującego anonimowość pomoże skoordynować się grupie także poza nim.

Rzeczywista demokracja przyszłości

Poszukiwanie nowych metod współdziałania społecznego jest spowodowane brakiem transparentności centralnych systemów – do których oczywiście należą organy i instytucje państwowe. Nie bez powodów zawsze doszukujemy się w nich korupcji i upolitycznienia, a samą politykę uważamy za brudną. Co gorsza, wydaje się, że wszelkie afery i konflikty wzmacniają polityków, zamiast ich dyskredytować.

Odpowiedzią na te bolączki jest system neutralny i audytowalny. Chcemy również, żeby był wydajny i rozwiązywał problemy efektywniej niż ten dotychczasowy.

Wszystkie wymienione zastosowania potrzebują wspólnej platformy, która koordynuje, uwierzytelnia, chroni i anonimizuje komunikację całego społeczeństwa. Myślę, że w przyszłości będzie nią blockchain. Działające w nim smartkontrakty będą funkcjonować według jasno określonych zasad, uzgodnionych przez wszystkie strony.

Mimo że blockchain określany jest mianem platformy zaufania, bazuje na braku konieczności ufania jakimkolwiek sędziom czy strażnikom. Formalizuje jedynie zasady i je bezwzględnie egzekwuje.

W blockchain jest wbudowany mechanizm regeneracji. Gdy zaobserwujemy jakikolwiek niepożądany efekt działania systemu, będziemy dysponowali wszelkimi danymi, które pomogą pchnąć jego ewolucję na właściwe tory.

Blockchain to platforma o niesamowitej płynności, udostępniająca rozliczne mechanizmy zachęty i katalizatory pożądanych aktywności, w tym realizowania wielu nowych, z natury zdecentralizowanych idei.

Blockchain, w połączeniu z ustrojami takimi jak płynna demokracja czy liberalny radykalizm, może naprawić politykę. Może stworzyć nowy, wspaniały demokratyczny świat.

---

* Sunoo Park, Michael Specter, Neha Narula, Ronald L. Rivest, *Going from bad to worse: from Internet voting to blockchain voting*, „Journal of Cybersecurity", Volume 7, Issue 1, 2021, doi.org/10.1093/cybsec/tyaa025 (data dostępu: 10.10.2022).

** Vitalik Buterin, Zoë Hitzig, E. Glen Weyl, *Liberal Radicalism: A Flexible Design For Philanthropic Matching Funds*, grudzień 2018, dx.doi.org/10.2139/ssrn.3243656 (data dostępu: 10.10.2022).

*** Bliźniaczym projektem jest Indiegogo (przyp. red.).

15

Sztuczna inteligencja

Sztuczna inteligencja i kryptowaluty to jedne z najgorętszych tematów ostatnich lat. Z tego powodu często trafiają do tego samego worka. Łączy się je w telewizji śniadaniowej i na ulotkach reklamujących studia. Sztuczna inteligencja i kryptowaluty wydają się wzajemnie tajemniczo przenikać, co sprawia wrażenie, że wspólnie tworzą jakieś monstrum. A że nie do końca wiadomo, czy są dobre jako oddzielne twory, to co dopiero powiedzieć o takim zespoleniu rodem z dystopijnej powieści popularnonaukowej?

Spróbujmy zatem rozprawić się z tą kwestią i przekonajmy się, czy sztuczna inteligencja (*Artificial Intelligence*, AI) ma w ogóle jakikolwiek związek z blockchainem i kryptowalutami.

Sztuczna inteligencja jest gałęzią rozwoju technologii, która zajmuje się imitacją działania ludzkiej inteligencji. By osiągnąć ten cel, korzysta z wielu dziedzin, takich jak przetwarzanie języka naturalnego, rozpoznawanie obrazów, gromadzenie i analiza dużej ilości danych. Kluczowym komponentem funkcjonowania systemów sztucznej inteligencji jest samouczenie się, nazywane często uczeniem maszynowym. Obecne systemy AI z powodzeniem analizują mapy, automatyzują zadania i coraz

bardziej wspierają ludzi lub nawet ich zastępują. Sztuczna inteligencja wkracza coraz śmielej w obszary zarezerwowane dotąd wyłącznie dla człowieka i jego abstrakcyjnego myślenia: mówię tu o sztuce. AI potrafi tworzyć muzykę czy grafiki na podstawie (słownego!) opisu tematu, stylu i innych charakterystycznych cech przyszłego dzieła. To naprawdę zdumiewające!

A czym są kryptowaluty? Dla porządku przypomnę: kryptowaluty to elektroniczne monety, które stanowią mechanizm koordynacji blockchaina – platformy pozwalającej na zawieranie umów elektronicznych, zwanych smartkontraktami. Połączenie umów i monet pozwala tworzyć ekonomię elektroniczną. Blockchain działa na danych dostarczonych przez użytkowników, gwarantując im niezależność, a wiarygodność i bezpieczeństwo przechowywanych w nim transakcji to warunek jego poprawnego działania.

Cóż, ja osobiście nie dostrzegam tu zbyt wielu wspólnych cech. Wiadomo, że i kryptowaluty, i AI do działania potrzebują komputerów…

Tak bardzo się różnimy…

Nie poddawajmy się i spróbujmy znaleźć wspólny mianownik tych dwóch fenomenów. AI i kryptowaluty to technologie przyszłości. Czy mogą się wspierać, korzystając z siebie nawzajem? Czy ścieżki ich rozwoju gdzieś się przetną? Zbiegną się? Czy w ogóle możemy zestawiać AI i kryptowaluty w jakimkolwiek kontekście?

Owszem. Obie platformy działają, opierając się na danych i przetwarzając ich olbrzymie ilości. Dane to dla nich plastyczna masa,

którą bez ustanku mielą, obrabiają i interpretują. To wielkie podobieństwo obu systemów, ale zarazem ich największa różnica!

Aby systemy uczenia maszynowego sztucznej inteligencji mogły optymalnie działać, potrzebują gigantycznej ilości scentralizowanej informacji. Takie dane inicjują procesy interpretacyjne i to na ich podstawie powstają narzędzia analityczne, jak na przykład sztuczne sieci neuronowe.

Jak działa uczenie maszynowe? Posłużę się pewną metaforą. Wyobraźmy sobie, jak w jakimś wyimaginowanym świecie wyglądałby proces wynalezienia… śrubokręta. Załóżmy, że istnieje zaawansowana robotyczna cywilizacja oparta na sztucznej inteligencji, która w ogóle nie korzysta ze śrubokręta. W ich robotyczne… macki? chwytaki? trafia stworzony na naszej planecie artefakt, zmontowany klasycznie, „po naszemu", czyli skręcony śrubami. Roboty chcą rozebrać go na części, ale nie wiedzą, jak to zrobić. Ich sieć neuronowa musi stworzyć odpowiednie narzędzie. Proces maszynowego uczenia się polega w tym przypadku na losowym doborze kształtów i sprawdzaniu, czy da się nimi usunąć śruby. Po milionach prób sieć neuronowa odkrywa, że śruby trzeba wykręcić (nie da się ich wyrwać!) i że potrzebne są do tego pręty, ale specyficzne: zakończone wąską, spłaszczoną końcówką. Efekt? Prawie wszystkie śruby odkręcone! Ale jedna się nie poddaje. Nowo wynalezione narzędzie przypominające ludzki śrubokręt ślizga się na niej – no tak, śruba z wgłębieniem imbusowym. Niepowodzenie wymusza na sieci neuronowej kolejne próby i po jakimś czasie – teraz już znacznie krótszym, bo modyfikacja narzędzia polega na modyfikacjach końcówki, która do tej pory się sprawdzała – w zbiorze danych pojawia się klucz imbusowy.

W realnych zastosowaniach zbiór informacji systemu sztucznej inteligencji musi być olbrzymi. Aby autonomiczny samochód był bezpiecznie prowadzony przez autopilot, potrzebne są miliardy symulacji

i testów. Gdy dane służące do nauki nie będą wystarczająco różnorodne, autopilot nie zadziała w każdej możliwej sytuacji. Gdyby robotom z naszego przykładu nie przydarzyła się śruba imbusowa, ich system AI nie zdołałby jej szybko odkręcić przy innej, późniejszej okazji. Musiałby wynaleźć imbus praktycznie od zera.

To, że do działania AI potrzeba olbrzymiej bazy danych, jest źródłem poważnych kontrowersji; takie szczegółowe dane mogą zostać użyte w dobrym celu, ale także w celu etycznie wątpliwym. Wykorzystując AI i dane, można opracować kształt wytrzymalszego skrzydła samolotu lub łatwo wykryć przestępstwa finansowe. Ale można też odkryć najlepszy sposób prezentacji reklam, by zwiększyć sprzedaż jakiegoś produktu. A nawet i to nie jest takie złe – o wiele gorsze jest bowiem wykorzystanie danych do wpływania na zachowania całych społeczeństw (nieodmiennie polecam książkę *Mindf*ck* Wyliego). Tym bardziej, że zdarza się, iż dane do takiej bazy gromadzone są bez zgody i wiedzy ich właścicieli.

Widać wyraźnie, że AI pod względem podejścia do danych to zupełne przeciwieństwo blockchaina. Blockchain opiera się na decentralizacji informacji. Mimo że jest często rozumiany jako wspólna, publiczna baza danych, to dane te nie muszą być ze sobą połączone, by zapewniać jego działanie. Blockchain bardziej przypomina wyspy danych, między którymi podróżują użytkownicy.

Miliarder z Doliny Krzemowej i założyciel PayPala Peter Thiel zasłynął z porównania filozofii działania sztucznej inteligencji do komunizmu, a blockchaina – do libertarianizmu. Jest to dość radykalna metafora, ale całkiem trafnie punktuje niebezpieczeństwo centralizacji dużej ilości danych.

A jednak się lubimy…

Czy w związku z tym sztuczna inteligencja i kryptowaluty są na kursie kolizyjnym? Otóż nie! Istnieje sporo obszarów, gdzie te dwie technologie mogą się uzupełniać, by jeszcze lepiej się rozwinąć.

Kontrowersyjnym tematem, do którego często wracam, są media społecznościowe. Wiele mówi się o manipulacji zachowaniem użytkowników portali społecznościowych. Podpowiadane treści, wyświetlane pod dyktando algorytmów sztucznej inteligencji, są tak dobrane, by wywołać jak największe emocje i doprowadzić do jeszcze silniejszego zaangażowania w materiały dostępne na portalu. Było to świetnie pokazane w popularnym na Netfliksie filmie *Dylemat społeczny*. Twórcy portali oczywiście zaprzeczają, że to celowe działanie, i zapewniają, że ich głównym zamiarem jest łączenie ludzi, a nie sprzedaż reklam. Lecz jak to zweryfikować?

A gdyby tak wymagać, by algorytmy podpowiadające treści były smartkontraktami? Jako kod zapisany w blockchainie byłyby całkowicie jawne i weryfikowalne. Nie musielibyśmy ufać właścicielom portali co do ich intencji. W blockchainie – publicznej bazie danych – moglibyśmy wszystko sprawdzić samodzielnie. No, może to odrobinę za dużo powiedziane, że „wszystko” i „samodzielnie” – trudno jest weryfikować działanie skomplikowanych algorytmów, niemniej stosunkowo łatwo można by ocenić, czy ktoś przypadkiem nie zaingerował w ich autonomiczne działanie.

Gdyby doszło do próby manipulacji, na przykład podczas kampanii wyborczej, moglibyśmy łatwo sporządzić elektroniczny dowód tego, że dane, które widzimy, albo są zmanipulowane (co byłoby widoczne

w smartkontrakcie), albo nie są wyświetlone za pośrednictwem smartkontraktu (co świadczyłoby o złamaniu zasad).

Myślę, że takie zintegrowanie blockchaina z systemami sztucznej inteligencji mediów społecznościowych oddałoby trochę władzy użytkownikom i korzystnie wpłynęło na nasze życie społeczne.

A w drugą stronę? Czy AI może pomóc blockchainowi?

Oczywiście. To dzieje się już teraz. Wykorzystujemy fakt, że blockchain jest publiczną bazą danych, którą możemy analizować. Użytkownicy są w nim co prawda pseudoanonimowi, ale blockchain rejestruje ich interakcje. Systemy uczenia maszynowego pozwalają wytropić próby przestępstw i oceniają wiarygodność użytkowników.

Innym obszarem synergii sztucznej inteligencji i kryptowalut jest sieciowy charakter blockchaina. Naukowcy i badacze z najróżniejszych dyscyplin mają często kłopot ze znalezieniem niezależnych, wiarygodnych i różnorodnych danych. To istotny problem, który spowalnia badania choćby w przemyśle czy farmacji. Blockchain – dzięki temu, że jasno określa sposób komunikacji i uzgodnienie prawdy w sieci – może „zawędrować” o wiele dalej i zebrać o wiele więcej ciekawej wiedzy niż systemy scentralizowane, przed którymi nauczyliśmy się bronić i którym nie ufamy. Ten przykład jest mi bardzo bliski: na studiach zajmowałem się uczeniem maszynowym. Nasz system ewoluował sieci neuronowe na niezależnych wyspach – tak zwanych agentach. Myślę, że takie systemy sztucznej inteligencji mogłyby rozwinąć się w bardzo obiecującym kierunku, mając do dyspozycji różnorodne dane węzłów sieci blockchain, działających jak wyspy.

Zaczęliśmy ten rozdział od dwóch gorących tematów, a zakończymy go trzecim – równie gorącym. NFT. Jak dobrze wiesz, artyści mogą stać się beneficjentami tej technologii. Pisałem wcześniej o tym, jak mogliby

wpływać na losy swojego dzieła już po sprzedaży i tworzyć zaczyn do kreacji kolejnych losowych dzieł. Dzięki temu, że odbywa się to w sposób ustandaryzowany, poprzez smartkontrakt NFT, powstaje wspólna baza interakcji miłośników sztuki, dzieł i twórców. Sztuczna inteligencja może przyjść tutaj z oszlifowanymi w mediach społecznościowych algorytmami reklamowymi i zasugerować entuzjastom sztuki, co jeszcze mogłoby się im spodobać. Takie algorytmy działają, korzystając z publicznych danych, a ich wynik jest odczytywany tylko przez zainteresowane strony – to chyba najbardziej etyczna wersja targetowanej reklamy.

Post- i inter-

Na zakończenie tego rozdziału pokuszę się jeszcze o inny sposób sformułowania różnicy między blockchainem a sztuczną inteligencją. Sztuczna inteligencja – ze względu na przyświecający jej cel – ma charakter postczłowieka, jest niejako postludzka. Jej zadanie polega przecież na zastąpieniu człowieka wszędzie tam, gdzie sprawdzi się lepiej od niego. Natomiast celem blockchaina jest usprawnienie działania między ludźmi, przeniesienie interakcji na wyższy poziom. Można zatem powiedzieć, że blockchain ma charakter interludzki. W żadnym wypadku nie chcę tu wartościować tych jakże odmiennych technologii – obie są w naszych rękach i to od nas zależy, jak z nich skorzystamy. Wydaje mi się jedynie, że przedrostki „post-” i „inter-”, zestawione ze słowem „człowiek”, znakomicie oddają istotę sztucznej inteligencji i blockchaina. Postczłowiek i interczłowiek… Współpraca czy konflikt? A jeśli konflikt, to kto ma większe szanse na zwycięstwo?

Sztuczna inteligencja i kryptowaluty – cóż to za koktajl! Te dwie technologie różnią się, ale i dopełniają. Oby pomogły sobie nawzajem – splatając się w wyrafinowany sposób, zyskają moc, by wyeliminować swoje największe wady.

16

Kryptorozmaitości

Chciałbym ci teraz zaproponować chwilę rozrywki. Rozłóżmy na czynniki pierwsze niektóre z naszych codziennych aktywności i na podstawie tego, czego do tej pory dowiedzieliśmy się o blockchainie, sprawdźmy, jak by się zmieniły, gdyby włączyć go do gry.

E-mail

Być może zastanawiałeś się, dlaczego spam – czyli niechciane maile – w ogóle istnieje. Po co to komu? Przecież i tak nikt ich nie czyta i nie klika w zaszyte w nich linki, prawda? No… to nie takie proste. Spam rozsyłany jest w wielkich kampaniach mailowych obliczonych dosłownie na miliardy wiadomości. Przy takiej ich liczbie nawet ułamek promila odbiorców klikających nieopatrznie w zawarty w nich link wygeneruje potencjalny zysk dla nadawcy. Spam jest też głównym kanałem „wstrzykiwania” wirusów przejmujących nasze komputery, hasła, dostępy do kont w mediach społecznościowych czy w bankach. Częściowo uporaliśmy się z tym problemem dzięki skutecznym filtrom antyspamowym. Im większa

jest firma świadcząca usługi hostingowe, tym lepiej odsiewa niechciane maile, bo dysponuje ich szerokim przeglądem. Ale to wyścig zbrojeń. Nadawcy spamu zawsze mają jedną odpowiedź: „Więcej spamu. Jeszcze bardziej pomysłowego, jeszcze groźniejszego”.

Istnieje bardzo prosty sposób walki ze spamem – właśnie dzięki technologii ze świata blockchaina. Zaproponowali go wynalazcy protokołu Dowodu Pracy (*Proof of Work*) na początku lat dziewięćdziesiątych ubiegłego wieku: Cynthia Dwork i Moni Naor. Wystarczy do każdej wiadomości dodać kryptozagadkę, ale nie tak trudną, jak ta zastosowana przez Satoshiego Nakamoto przy kopaniu bitcoina.

Szczegóły tej metody opisał Adam Back w pracy *Hashcash*. Nadawca, zużywając choćby część sekundy, by rozwiązać zagadkę kryptograficzną dołączoną do każdego wysyłanego maila, będzie sparaliżowany czasowo – musi bowiem robić to miliard razy przy wysyłce całej kampanii spamowej. Dla zwykłego człowieka czas potrzebny komputerowi do rozwiązania jednej zagadki to dosłownie mrugnięcie okiem. Ale miliard sekund potrzebnych do rozwiązania miliarda zagadek, to… prawie 32 lata!

Jak wiemy, takie „kopanie”, czyli rozwiązywanie kryptozagadek zużywa zasoby naturalne (potrzebujemy prądu i mocy obliczeniowej!). Owszem, jednak zawsze musimy spojrzeć na drugą stronę medalu. Miliardy niechcianych maili obciążają łącza i serwery, przyczyniając się do marnotrawstwa energii – kto wie, czy nie zużywają jej więcej niż kryptoobliczenia. A utrudniając nam wszystkim pracę i narażając na oszustwa internetowe, wpływają negatywnie na wydajność i jakość życia. Nie mówiąc już o tym, że jeśli w zagadce kryptograficznej zawrzemy część jakiegoś ważnego obliczenia, to przy wysyłce maili serwery mogą rachować coś, co przydaje się ludzkości.

Niestety, jak dotąd rozwiązanie z *Hashcash* nie jest stosowane. Głównym powodem braku jego implementacji były obawy, jak uczciwi nadawcy, rozsyłający wartościowe newslettery, poradzą sobie z tym zagadnieniem. Pamiętajmy, że na przełomie wieków e-mail był krwiobiegiem internetu. Obecnie, w czasach czatów, wideokonferencji i metawersów, rola e-maili jest zupełnie inna. Może *Hashcash* będzie prostym sposobem, by uszlachetnić ten środek komunikowania się w internecie?

Sieci społecznościowe

Sieci społecznościowe to wynalazek ostatnich lat. Facebook powstał w 2004 roku, Twitter dwa lata później. Można by zażartować, że obecnie platformy te są ledwie pełnoletnie, a już pokazały, jak zdestabilizować świat dorosłych! Po bardzo kontrowersyjnych wyborach prezydenckich w USA i referendum brexitowym wiele się mówi o polaryzowaniu społeczeństw przez serwisy społecznościowe. Jednym z narzędzi wpływu jest niemal darmowe tworzenie fałszywych tożsamości w tym wirtualnym świecie. Potem armie botów – lub trolli – manipulują opinią publiczną, wpływając na wyniki plebiscytów i niszcząc tkankę społeczną. Niektórzy twierdzą nawet, że to nowa forma wojny hybrydowej, i nie sposób odmówić im racji.

Może sam już dostrzegasz, jak rozwiązać ten problem. Jak sprawić, żeby utworzenie nowego profilu na naszym ulubionym portalu społecznościowym nie było tak łatwe i szybkie? Oczywiście na pomoc znów przychodzi Dowód Pracy. Zakładanie profilu społecznościowego to sprawa większej wagi niż wysłanie e-maila. Może kryptozagadka, która ma zostać rozwiązana przy konfiguracji nowego konta, powinna się obliczać

cały dzień? Z pewnością pomogłoby to w ograniczeniu armii trolli, dolewającej oliwy do ognia w praktycznie każdej dyskusji w internecie…

Reklamy w internecie

Czy nie irytuje cię przeklikiwanie po raz setny zgód na reklamy? Albo instalacja najnowszego programu, który je blokuje, za każdym razem, gdy zmieniasz laptop lub przeglądarkę? Bez takich „adblockerów” darmowe strony internetowe wyglądają jak wielki śmietnik, skutecznie rozpraszając naszą uwagę, już i tak nadwerężoną śledzeniem wątku z tekstem, który usiłujemy przyswoić.

Podobnie jak w przypadku spamu, celem jest skłonienie nas do kliknięcia w zaszyty w reklamie link. Właściciele serwisu otrzymują zapłatę za kliknięcia, które wygenerował ich portal. Sprawdza się tu stare przysłowie: jeśli dostajesz coś za darmo, to znaczy, że to ty jesteś towarem.

Reklamy, które nas atakują w internecie, nie są przypadkowe. Są do nas dokładnie dobrane na podstawie historii odwiedzin stron internetowych, i to nie tylko naszych, ale także naszych bliskich. Dane o zainteresowaniach, preferencjach i rzeczach, którym poświęcamy uwagę, są zatrważająco kompletne i wielokrotnie przemielone najnowocześniejszymi algorytmami uczenia maszynowego. Przez ten ułamek sekundy po wpisaniu adresu lub kliknięciu w link prowadzący do strony, którą chcemy otworzyć, jeszcze zanim się ona wyświetli, trwa zacięta bitwa – bitwa o nas. Jej zwycięzcą jest ten, kto odkryje, kim tak naprawdę jesteśmy i czym się interesujemy. To zwycięzca zalicytował nieco więcej w aukcji o miejsce reklamowe. Wobec reklamy dedykowanej dokładnie nam jesteśmy praktycznie bezbronni. Nawet jeśli nie zdajemy sobie z tego sprawy, rezonuje ona z mechanizmami

działającymi głęboko w naszym umyśle. I niejednokrotnie przełoży się na decyzję o dokonaniu zakupu.

Czyli… to niezbyt etyczne?

Owszem, ale niepłacenie za treści też nie jest etyczne. Utrzymanie portalu to wielkie koszty. Zespół, serwery, treść. Obecnie reklama to jedno z niewielu źródeł dochodu, które pozwala ją utrzymać się na powierzchni bardzo wartościowym serwisom.

Gdzie szukać rozwiązania? Co da się zrobić? A gdyby do naszej przeglądarki internetowej dołączyć specjalny portfel z kryptowalutą? Zawierałby niewielkie środki, takie podręczne kryptowalutowe drobniaki. Wydawalibyśmy je przy każdym kliknięciu na stronie i z każdym wczytaniem podstrony. Każde takie kliknięcie to ułamek grosza. Reklamodawcy wyceniają je tak nisko, że liczą je w paczkach po dziesięć tysięcy.

Z tego samego portfela płacilibyśmy również bezpośrednio za treści. Bez konieczności kupowania abonamentu i bez podawania danych karty kredytowej. Konsumpcja treści w internecie przestałaby oznaczać, że wydajemy kilkadziesiąt złotych miesięcznie na abonamenty na kilkunastu portalach – zwykle przecież i tak zaglądamy tylko do części z nich, z reguły po to, by przeczytać interesujący nas artykuł (a nie, by zapoznać się z kolejnym numerem magazynu w całości). Płacilibyśmy tylko za te treści, które rzeczywiście czytamy.

Takie rozwiązanie jest możliwe tylko dzięki kryptomonetom i ich zdecentralizowanemu charakterowi. Gdyby portal za każdym razem, gdy korzystamy z zamieszczonych na nim treści, musiał obciążać naszą kartę płatniczą jakąś drobną kwotą, nie miałoby to sensu: sama obsługa płatności okazałaby się droższa niż dostęp do artykułu. Systemy kryptowalutowe nie korzystają z takiego karkołomnego systemu mikropłatności jak tradycyjne

banki z ich kartami kredytowymi. W świecie kryptowalut i blockchaina wraz z kliknięciem automatycznie przesyłamy dowód zapłaty, który zawiera wszystkie potrzebne do dokonania transakcji dane. Dowód, który – jak wszystko w blockchainie – jest nienaruszalny i niepodrabialny. Może zatem doczekamy się jeszcze internetu bez reklam? I wartościowych, a nie clickbaitowych treści?

Rozrywka

Blockchain zmieni nie tylko negatywne aspekty internetu. Pozwoli także inaczej doświadczać w nim przyjemnych chwil.

Gaming

Gry wideo już od dawna wprowadzają do rozgrywek elementy ekonomii. Spora ich część jest darmowa – ale płaci się za skórki, przedmioty, eliksiry czy lepszą broń; czasem bez tych wirtualnych przedmiotów (lub dodatkowych mocy) zakupionych w grze rozgrywka staje się bardzo trudna, wręcz niemożliwa.

Gdybyśmy taką wewnętrzną ekonomię gry oparli na blockchainie, zapewnilibyśmy sobie większe bezpieczeństwo. Sprawdzona kryptografia skutecznie chroniłaby naszą wirtualną własność i osiągnięcia – obecnie wszelkie informacje związane z rozgrywką, stopniem jej zaawansowania i stanem posiadania graczy są tylko zapisem w bazie danych, który w każdej chwili – w wyniku splotu jakichś niefortunnych okoliczności – może zniknąć.

Innym aspektem wprowadzenia kryptowalut do rozliczeń w grze jest łatwość migracji monet między niepowiązanymi ze sobą uniwersami.

Studio gier wydające wiele tytułów mogłoby korzystać z jednej waluty – wówczas bez problemu spieniężylibyśmy miecz w jednej grze i za pozyskane środki kupilibyśmy silnik do promu kosmicznego w innej. Myślę, że takie rozwiązanie bardzo by ułatwiało skupianie społeczności graczy wokół jednego studia.

Zróbmy jeszcze jeden krok w głąb świata blockchaina.

W grach komputerowych korzystamy z rozmaitych wirtualnych przedmiotów, które zapewniają nam przewagę lub pozwalają doświadczać wirtualnego świata w jakiś niestandardowy sposób. Najnowszy trend w grach, które wykorzystują blockchain, to reprezentowanie osobistego inwentarza przez tokeny NFT. Mają one charakter kolekcjonerski, są też bardzo drogie. Ich ceny sięgają kilku, a czasem nawet kilkunastu tysięcy dolarów. Tak oto powstaje kolejna warstwa ekonomii: elementy inwentarza, będące tokenami NFT, są wypożyczane przez właścicieli uzdolnionym graczom. Jest to model Play-To-Earn, czyli „graj, by zarabiać”. Gracze biorą udział w rozmaitych zawodach i turniejach, wygrywając nagrody pieniężne. Pochodzącymi z nich środkami opłacają właściciela wypożyczonego sprzętu, który przecież w jakimś stopniu zapewnił im zwycięstwo. Ze wzmożonej aktywności w tej dziedzinie słyną kraje południowo-wschodniej Azji, w szczególności Filipiny. Rozwój metawersów, o których pisałem w rozdziale poświęconym NFT, będzie jeszcze bardziej dynamizował tę gałąź rozrywki.

Blockchain w grach? Zarobią na tym gracze, zarobią właściciele NFT, zarobią twórcy gier.

Całkowite zanurzenie i kryptokotki

Istnieją gry zawarte w całości w smartkontraktach. Był czas, że straciły na popularności – okazało się, że opłaty za dokonywane w nich transakcje są

zbyt wysokie. Powróciły do łask wraz ze wzrostem wydajności systemów i pojawieniem się możliwości tworzenia wielu nowych, niezależnych platform. Co to za gry?

Bardzo ciekawe! Pierwszą z nich były *Cryptokitties* – czyli kryptokotki. Zasada działania kryptokotków jest obecnie powielona w różnorakich kolekcjonerskich tokenach NFT. Jak już dobrze wiesz, token NFT to część smartkontraktu w blockchainie. Gdy zawrzemy w nim pewien element losowości, stworzymy ciekawą grę.

Oto, jak to działa.

Kolekcjonujemy tokeny. Możemy ich użyć do stworzenia nowych tokenów. Mechanizm najlepiej zrozumieć na przykładzie kryptokotków: parujemy kotki i z tego sparowania rodzą się im dzieci. Zarówno kotki-rodzice, jak i kotki-dzieci mają DNA, które jednoznacznie identyfikuje ich rodzinną relację. DNA kryptokotków koduje kilkanaście ich cech, takich jak kształt oczu, kolor sierści i tym podobne. Celem hodowli kryptokotków jest otrzymanie zwierzęcia o wybitnie rzadkich i bardzo pożądanych cechach. Ceny wyjątkowych kotków osiągają niezwykle wysoki pułap. Wartość najcenniejszych kryptokotków może przekroczyć… sto tysięcy dolarów! Motywuje to graczy do ciągłych prób.

Element losowości został powtórzony w wielu innych tokenach NFT. Przykład ze świata sztuki: artysta w swoich dziełach, które są tokenami NFT, może zawrzeć ściśle określony mechanizm losowości, który w zadany przez niego sposób będzie wpływał na kolejne generacje jego dzieł. Łączy to reprodukcję dzieła z jego unikatowością.

Kasyno

Jak zorganizowałbyś kasyno w blockchainie? Pytanie wydaje się trochę nie na miejscu… Lecz cyfrowy pieniądz aż się prosi, by używać go do gier

hazardowych. Pozostaje tylko kilka wyborów, których musimy dokonać. Możemy stworzyć własną kryptowalutę, własny smartkontrakt lub pozwolić graczom na używanie dostępnych par walutowych. Własna waluta może pomóc finansować serwis internetowy kasyna (w analogii do kryptowalutowej wypożyczalni Karola, pamiętasz?). Zastosowanie istniejącej już kryptowaluty mogłoby zapoczątkować budowanie większego ekosystemu rozrywek hazardowych, czegoś w rodzaju wirtualnego Las Vegas. Użytkownicy z łatwością mogliby zmieniać domy gry, nie ponosząc przy tym kosztów przewalutowania.

Dużą zaletą blockchainowej obsługi gier hazardowych z punktu widzenia graczy jest to, że ich środki byłyby chronione przez ich własne portfele kryptowalutowe. Nie powtórzyłaby się wówczas sytuacja sprzed paru lat, kiedy to w wiodących pod względem popularności hazardu krajach firmy pokerowe zostały zmuszone do zamrożenia kont użytkowników.

Zakłady

Blockchain i klasyczne zakłady? Nic prostszego. Dowolny serwis publikuje dostępne zakłady. Fani wszelkich sportów (i innego typowania) po podłączeniu portfela kryptowalutowego mogą obstawiać kryptowalutą preferowane wyniki. Ewentualne wygrane wędrują wprost do nich.

A skąd smartkontrakt uzyskuje informacje, który z obstawianych zespołów lub sportowców (czy polityków lub ugrupowań, jeśli obstawiamy wyniki wyborów) wygrał i którym graczom trzeba przelać środki? Oczywiście korzysta z mechanizmu wyroczni, który przekazuje wyniki zmagań do blockchaina, po czym używa tych danych, by wyznaczyć wygrywającą stronę zakładu.

17

Waluta rezerwowa

Nasze życie codzienne to nie inwestycje w NFT, nabywanie i sprzedawanie nieruchomości czy powoływanie spółek przy pomocy smartkontraktów. To kupowanie biletu na tramwaj. Pośpieszna kawa po lunchu w pracy. Opłata za przejazd autostradą. Jak wyrazić ceny tych dóbr w kryptowalutach – pieniądzach, których kurs jest tak… rozchwiany? Kryptowaluty kojarzą się bowiem z dużą niestabilnością – w ciągu zaledwie jednej doby mogą zyskać lub stracić na wartości nawet kilkadziesiąt procent! To istny magnes na spekulantów. Niestety obietnica szybkich zysków przyciąga zmanipulowanych kupujących, którym wydaje się, że są inwestorami, podczas gdy ich działania bardziej przypominają grę w ruletkę. Zastanówmy się zatem, jak moglibyśmy używać kryptowalut na co dzień. Czy w ogóle da się korzystać w najpowszedniejszych sprawach z pieniądza, którego wartość zmienia się dosłownie z minuty na minutę?

Stablecoin

Odpowiedzią na te potrzeby są waluty stabilne (*stablecoins*). Jednostka monetarna takiej waluty deklaruje, że zawsze będzie miała stałą wartość – stałą w sensie stałości klasycznych walut. Ponieważ w rozliczeniach międzynarodowych dominują zachodnie potęgi gospodarcze, kursy najpopularniejszych walut stabilnych podążają za dolarem amerykańskim.

Jak w ogóle jest możliwe takie „dowiązanie się" do klasycznych walut? Istnieje kilka metod realizacji tego zadania.

Tether

Najbardziej znana metoda to zabezpieczenie wartości kryptowaluty aktywami w tradycyjnym świecie finansów. Przykładem takiego podejścia jest scentralizowana waluta tether (USDT). Partie waluty są „drukowane" w wirtualnym kontrakcie, który jest powiązany z zasobami firmy Bitfinex. Tether zobowiązuje się, że 1 USDT będzie zawsze wart 1 USD.

Wywołuje to oczywiście sporo kontrowersji. Powstają nawet teorie spiskowe, którym nie sposób odmówić pewnej racji – wytykają one tetherowi brak przejrzystej procedury utrzymywania oparcia waluty w aktywach lub wpływanie na cenę bitcoina. Przy czym audyt tego tworu wcale nie jest trywialnym zadaniem.

Tether ma obecnie wartość całkowitą około osiemdziesięciu miliardów dolarów. To zaś sprawia, że mimo wspomnianych zastrzeżeń, ta waluta stanowi kręgosłup finansowej domeny świata krypto.

Z tethera korzystamy wówczas, gdy nie jesteśmy gotowi na inwestycję naszych środków, ale nie chcemy być zależni od wahań kursów kryptowalut. Praktycznie każda większa giełda utrzymuje tak zwane pary walutowe (zestawienie dwóch różnych walut; wartość tego zestawienia jest

wyznaczona jako stosunek wartości walut w parze), w których jedną z walut jest właśnie tether.

Tether osiąga stały kurs walutowy i jest wymienialny w stosunku 1:1 na dolara – czyni to za pomocą pełnej rezerwy dolarowej w świecie rzeczywistym. Zasoby tethera, które mają to gwarantować, to 2,9% jego ogólnej wartości w gotówce i ponad 93% w bardzo bezpiecznych instrumentach finansowych o wysokiej zdolności kredytowej (w terminologii finansowej: o ratingu AA lub wyższym).

Tether to waluta stabilna z mechanizmem rezerwowym poza blockchainem (*off-chain*), opartym na pieniądzu fiducjarnym, czyli emitowanym przez bank centralny (w tym wypadku jest to dolar).

Czy w takim razie tether jest dobrą walutą, by wyrazić w niej cenę biletu autobusowego w Polsce? Niezbyt. Raczej nie powinniśmy uzależniać finansów naszego państwa od firmy trzeciej z siedzibą na Brytyjskich Wyspach Dziewiczych. Poza tym tether jest „dowiązany” do dolara, a przecież kurs złotówki do amerykańskiej waluty również się waha!

Ciekawostką jest, że w niektórych krajach obowiązek podatkowy z zysków obrotem kryptowalutami powstaje dopiero po „wyjściu” z kryptowalut do pieniądza fiducjarnego (takim krajem jest na przykład Polska). Jeśli zatem naszą zyskowną inwestycję zrealizujemy w Polsce w walucie tether, to całość „tetherowego” przychodu (bez uszczuplenia go o podatek) możemy wymienić na inną kryptowalutę, gdyby tego wymagała nasza kolejna inwestycja.

MakerDao

Bardzo ciekawą opcją są zdecentralizowane waluty rezerwowe z rezerwą *on-chain*, czyli w blockchainie. Zabezpieczenie takiej waluty to nie rzeczywiste aktywa i gotówka, lecz inne kryptowaluty.

Pierwszym i dotychczas jednym z popularniejszych projektów tego typu jest MakerDao. Jest to smartkontrakt, który emituje walutę dai podążającą za kursem dolara z wymianą 1:1. Można stać się jej posiadaczem, transferując do kontraktu MakerDao na przykład ether, czyli walutę blockchaina Ethereum, przy czym przelew musi opiewać na znacznie wyższą kwotę, niż wynikałaby ona z przelicznika ether/dolar: MakerDao zabezpiecza w ten sposób stabilność swojego kursu względem dolara. Obecnie tylko 2/3 wpłaconej w walucie ether kwoty jest wymieniana na dai; pozostała 1/3 to zabezpieczenie przed wahaniami rynku.

Zauważmy, że ponieważ wszystkie operacje związane z dai są zapisywane w blockchainie, audyt rezerw MakerDao jest bardzo prosty. Cena, jaką za to płacimy, to ryzyko technologiczne – polegające choćby na możliwości wystąpienia błędu w smartkontrakcie – oraz „kursowe” – łatwo sobie wyobrazić, co by się działo, gdyby wartość ethereum spadła wyraźnie poniżej granicy zabezpieczenia, na przykład z dwóch tysięcy do jednego dolara.

Wyrocznia

Smartkontrakt MakerDao (i w ogóle waluty rezerwowe) to znakomita okazja, aby porozmawiać o kolejnych standardowych narzędziach wykorzystywanych do budowy blockchaina.

Być może zastanawiasz się, skąd MakerDao uzyskuje dane o cenie ethereum. Mówi mu o tym pewien mechanizm, który „wstrzykuje”

informację ze świata zewnętrznego (*off-chain*) do świata blockchaina (*on-chain*). Zwie się on – jak na cyberpunkową stylistykę przystało – wyrocznią (*oracle*). Szczerze mówiąc, sam jestem zaskoczony, że o wyroczni mówimy dopiero teraz. To jeden z podstawowych elementów blockchaina: każda informacja ze świata ludzi, jeśli tylko jest wymagana do przeprowadzenia smartkontraktu, zapisuje się w blockchainie. Gdyby tak się nie działo i każdy kontrakt sprawdzałby we własnym zakresie ceny, temperatury czy wyniki meczów, to nigdy nie byłoby gwarancji, że wszyscy górnicy lub walidatorzy otrzymają w swoich obliczeniach ten sam wynik – mogliby przecież sprawdzić cenę jakichś aktywów minutę później… Wyrocznia jest łącznikiem świata zewnętrznego ze światem blockchaina. Zapewnia porozumienie i wspólne źródło prawdy dla wszelkich walidatorów.

Istnieje wiele przykładów stosowania wyroczni. Jeden z nich to kontrakty ubezpieczeniowe. Służą one automatycznemu wypłaceniu odszkodowania, gdy są spełnione określone warunki. Takie rozwiązanie przechodzi próbne testy w rolnictwie: gdy wyrocznia przekaże do blockchaina informację o wystąpieniu powodzi lub suszy na danym obszarze, ubezpieczeni rolnicy otrzymają automatyczną wypłatę ze stosownego smartkontraktu z polisą.

Samorządność

Drugim mechanizmem, na który chciałbym zwrócić uwagę przy okazji omawiania walut rezerwowych, jest samorządność aplikacji blockchaina. Zadajmy sobie pytanie: skąd wzięło się ustalenie, że zabezpieczenie kursowe MakerDao to 1/3, a nie na przykład 1/2 wpłaty? Czy wynika to z jakichś symulacji? Czy wyliczył to jakiś analizujący ryzyko algorytm?

Być może, ale ostatecznie zadecydowali o tym posiadacze prawa głosu w sprawie konfiguracji odpowiedniego smartkontraktu.

Otóż „DAO” w nazwie „MakerDao” oznacza zdecentralizowaną autonomiczną organizację (*Decentralized Autonomous Organization*). Działa ona, opierając się na wbudowanym w blockchain mechanizmie prowadzenia dowolnego przedsięwzięcia przez jego udziałowców lub po prostu użytkowników.

To często spotykane rozwiązanie określa się angielskim słowem *governance* (od greckiego *kubernaein* – sterować), rozumianym w świecie blockchaina jako „samorządność”. Wspólne podejmowanie decyzji ma olbrzymi, nieodkryty jeszcze do końca potencjał, który wynika między innymi z automatyzacji i koordynacji procesów wykorzystujących do działania publiczne dane.

Jak w MakerDao działa DAO?

Mechanizm samorządności może być wyrażony poprzez specjalne tokeny, które w przypadku MakerDao nazywają się skrótowo MKR. Może też opierać się na tych samych tokenach co waluta i podlegać zwykłym mechanizmom rynkowym. Tokeny MKR są ostatecznym zabezpieczeniem kursu dai, a w trybie normalnej płynności „obsługują” samorządność: wykorzystuje się je do głosowania nad wielkością zabezpieczenia lub na przykład nad tym, jaki inny kryptowalutowy token może stać się zabezpieczeniem „druku” waluty dai.

MakerDao jest zatem całkiem dobrym programowalnym smartkontraktem, którym możemy realizować obsługę sprzedaży biletów autobusowych. Co prawda waluta dai jest „dowiązana” do dolara, a nie do

polskiego złotego, jednak nic nie stoi na przeszkodzie, by pokonać to ograniczenie. Kod wszystkich smartkontraktów jest publiczny, a organizacja Maker publikuje całą dokumentację: można zatem stworzyć smartkontrakt podążający za polskim złotym.

Waluty algorytmiczne i krach Terry

Na koniec – niejako do kompletu – chcę wspomnieć o ostatniej kategorii kryptowalut. Jest ona najmłodsza, ale wyszła już z fazy eksperymentów. Omawialiśmy waluty z zabezpieczeniem poza blockchainem (*off-chain*), w blockchainie (*on-chain*), czas zatem na… stabilne waluty bez zabezpieczenia! To tak zwane waluty algorytmiczne.

Jak zatem realizowana jest stabilność takiego tworu? Otóż osiąga się ją poprzez manipulowanie parami walutowymi na zdecentralizowanych giełdach walut (DEX). Kontrolując podaż monety zgodnie z założonym protokołem, minimalnym kosztem możemy śledzić dowolną wartość waluty stabilnej.

O walutach algorytmicznych zrobiło się głośno wiosną 2022 roku. Niestety. Niestety – bo to właśnie one dodatkowo osłabiły rynek kryptowalut, który borykał się wówczas z wieloma problemami. Błąd obsługi waluty stabilnej terraUSD (UST), zbudowanej w blockchainie Terra, wywołał lawinowy kolaps kursu: wycena jednostki UST spadła z jednego dolara do tysięcznych części centa. Waluta wyszła poza zakres „zdrowych” parametrów algorytmu, co bezpowrotnie zniweczyło możliwość stabilizacji jej kursu. Straty wynikające z tego krachu szacuje się na około 98% wyceny Terry, czyli ponad 45 miliardów dolarów. Ponieważ UST jako waluta stabilna była wykorzystywana przez wielu ludzi jako

lokata oszczędności, jej katastrofa ekonomiczna spowodowała mnóstwo ludzkich dramatów.

Jak zatem w okresie dużej niestabilności zachowywały się inne kontrakty, takie jak MakerDao? Znakomicie. Można powiedzieć, że bardzo wydajnie stabilizowały cały system. Mechanizm zastawu MakerDao sprawiał, że zaciągane w nim pożyczki spłacano w pierwszej kolejności. Kurs dai przez cały czas pozostawał w stosunku 1:1 do dolara.

CBDC

CBDC to skrót, który możesz znać z internetu, a oznacza on *Central Bank Digital Currency*, czyli w tłumaczeniu: waluta cyfrowa banku centralnego. Te litery jak mało co podnoszą temperaturę dyskusji o kryptowalutach. Dlaczego?

Na początek trzeba wyjaśnić kilka spraw. Po pierwsze: waluta cyfrowa wcale nie musi opierać się na blockchainie. Może stać za nią jakiś inny cyfrowy system udostępniający pieniądze obywatelom.

Po drugie: trzeba powiedzieć, czym tak naprawdę jest bank centralny. To bank szczególnie uprzywilejowany przez rząd danego kraju. Zawiaduje walutą krajową i pełni funkcję instytucji odpowiedzialnej za działanie całego systemu bankowego.

Natomiast waluta do rąk obywateli trafia za pośrednictwem banków komercyjnych – takich jak te, których siedziby mijamy na ulicy.

Nietrudno sobie zatem wyobrazić, że wspomniany system bankowy – na który składają się między innymi rozrachunki międzybankowe oraz polityka fiskalna kraju – zamiast bazować na obecnym systemie informatycznym, obsługiwany jest przez blockchain. W poprzednich

rozdziałach poznałeś już niezaprzeczalne zalety blockchaina i z pewnością przeczuwasz, że zapewniłby on uniwersalną i w pełni wiarygodną platformę wymiany informacji (a co za tym idzie – pieniędzy) dla banku centralnego, banków komercyjnych i obywateli.

Jakie są zalety tego rozwiązania? A może ma ono jakieś wady? Przecież budzi kontrowersje!

Bank centralny jest bardzo ściśle powiązany z kreatorami i wykonawcami polityki monetarnej każdego kraju. To właśnie dlatego przeciwnicy pomysłu centralnej cyfrowej waluty obawiają się, że państwa sprawujące nad nią całkowitą kontrolę mogłyby powiązać zachowania obywateli z procesem tworzenia pieniądza.

Łatwość ustanawiania zasad, które obowiązują w blockchainie, mogłaby zachęcić władze do wprowadzania rozmaitych rozwiązań wpływających na życie ludzi i społeczeństw. Na przykład krajowa waluta mogłaby mieć… termin przydatności do użycia. Zupełnie jak produkty spożywcze. Jeśli wypłacane jako pensja środki miałyby ustawioną datę ważności, musielibyśmy je szybko wykorzystać, inaczej po zadanym w blockchainie czasie stałyby się bezwartościowe. Z jednej strony pobudzałoby to konsumpcję, z drugiej – skutecznie zniechęcało do oszczędzania. Nie osądzając, czy to dobry, czy zły pomysł, chciałbym zwrócić uwagę na coś innego: że przykład ten pokazuje, jaką moc inżynierii społecznej mają pieniądze, których właściwości można dowolnie programować.

Oczywiście to tyko spekulacje, jeden z wielu możliwych scenariuszy. Innym sposobem wykorzystania programowalnych pieniędzy mogłoby być skuteczne zrealizowanie za ich pomocą koncepcji bezwarunkowego dochodu podstawowego (BDP). Kwota wypłacona przez państwo jako BDP – zgodnie z założeniami tej idei – mogłaby być wykorzystana

wyłącznie na podstawowe życiowe potrzeby, edukację, system ochrony zdrowia i tak dalej. Nie pozwoliłaby natomiast na gromadzenie oszczędności lub kupowanie produktów spoza grupy niezbędnych.

Dużą zaletą wsparcia banku centralnego blockchainem byłaby możliwość transparentnego audytu całego systemu finansowego i realizacji założeń polityki monetarnej. W każdej chwili wiedzielibyśmy, ile pieniędzy tworzy państwowy sektor bankowy i jak nimi zarządza.

Sfera budżetowa mogłaby rozliczać się z samorządami państwową walutą elektroniczną. Dałoby to obywatelom dogłębny wgląd w koszty realizowanych inwestycji i wysokość transferów pieniężnych z budżetu centralnego do kasy samorządowej.

Pójdźmy nieco dalej – sama kontrola nad publicznymi pieniędzmi jest czymś pożądanym, ale nie tak ekscytującym, jak kolejny poziom zastosowania blockchaina i kryptowalut w administracji lokalnej i państwowej. Otóż część naszych podatków zasila tak zwany budżet obywatelski, który jest rozdysponowywany na określone inwestycje w wyniku głosowania obywateli. Gdyby wszystko odbywało się w blockchainie, budżet obywatelski mógłby być całkowicie elektroniczny i wyrażony smartkontraktem. Zapewniłoby to lepszą komunikację lokalnych społeczności z rządem; zoptymalizowałoby wspieranie sensownych, pożądanych przez lokalne wspólnoty projektów, a także odkrywanie nowych potrzeb. Pisałem o tym szerzej w rozdziale o kryptowalutach w kontekście demokracji.

Blockchain dzięki transparentności ułatwia wykrywanie malwersacji finansowych. Zapewnia rzecz jasna anonimowość, ale przepływy środków są możliwe do śledzenia. Te wzbudzające podejrzenia podlegałyby dalszej analizie. Mogłoby to posłużyć do walki z szarą strefą. Już teraz rozpisuje się dokumentację systemu, który mógłby monitorować podatek VAT. VAT-

coin – jego token – byłby odporny na wszelkie oszustwa podatkowe: „zgubiony” kontekst podatku, przekroczenie granicy państwa lub zmianę stawki. Kluczowe w systemie VAT-coin jest zintegrowanie aktywności finansowej na jednej platformie. Może to być monitoring faktur z VAT-coinem reprezentującym VAT, ale też stabilna waluta VAT-coin do jego rozliczania.

W kilku krajach wprowadzono już pieniądz CBDC – na przykład w Chinach i niektórych krajach Ameryki Łacińskiej. To będzie bardzo ciekawe: obserwować, jak nowa, państwowa, elektroniczna kryptowaluta wpływa na zachowanie władz, rządu, banku centralnego oraz jak oddziałuje na gospodarkę i wydajność systemu finansowego.

Trwają prace nad e-euro i fed-coinem. Wprowadzenie fed-coina (amerykańskiej państwowej kryptowaluty) planowane jest na lata 2030–2035; osobiście uważam, że to bardzo optymistyczny wariant. System o takim znaczeniu należy wdrażać etapami. Trzeba monitorować wydajność i błędy. Dopiero dobrze przetestowane i sprawdzone w praktyce rozwiązanie będzie mogło zastąpić walutę krajową. Ale przecież zdążyliśmy już zgromadzić pewne doświadczenie z dobrymi kandydatami na zamiennik dolara! Są nim oczywiście waluty stabilne, o których pisałem wcześniej. Twórcy systemu oficjalnej waluty krajowej mogą czerpać z lat doświadczeń waluty stabilnej, wymienianej na dolara zawsze w stosunku 1:1.

W naszej części świata elektroniczny pieniądz państwowy testuje się w rozrachunkach międzynarodowych. Używają go na przykład Banque de France i Swiss National Bank.

Bank Rozrachunków Narodowych szacuje, że aż 90% banków centralnych bada możliwość wprowadzenia waluty cyfrowej. Już dziś pojedyncze kraje stosują to rozwiązanie. Funkcjonuje chociażby sand dollar

z Bahamów, który jest powiązany z oficjalną walutą kraju i można nim płacić podatki. Kambodża i Nigeria to kolejne kraje z oficjalną walutą cyfrową. Zarysowuje się tu pewne podobieństwo do poprzedniego etapu ewolucji w bankowości, gdy nowa generacja technologii w pierwszej kolejności została zastosowana przez kraje rozwijające się (w tym Polskę).

Co sprawia, że państwowa kryptowaluta wciąż nie jest powszechnie stosowana? Przyczyn jest wiele. Przede wszystkim z CBDC – przynajmniej na razie – jest związane ryzyko czysto technologiczne (błędy w oprogramowaniu, wydajność systemu). Inny powód może się wydać trochę zaskakujący – jest nim… sektor banków komercyjnych. Podejrzewam, że banki komercyjne będą tu wielkim hamulcowym. Dlaczego? Otóż państwowa kryptowaluta zarządzana smartkontraktami udostępni pożyczki, kredyty i inwestycje całkowicie w ramach swojego systemu – w pełni cyfrowego, bezpiecznego i wiarygodnego, z jasnymi i automatycznie stosowanymi zasadami. Banki komercyjne staną się wówczas kosztowym elementem układanki, tak naprawdę całkowicie zbędnym. Oczywiście można zorganizować obieg pieniądza tak, by banki komercyjne były potrzebne, ale taki system byłby sztuczny.

Zresztą nawet obecnie banki komercyjne nie realizują swojej misji zbyt wydajnie. Poziom ubankowienia wielu rejonów świata, szczególnie tych biedniejszych, jest bardzo niski. W Ameryce Łacińskiej migracja sektorów państwowych do blockchaina i kryptowalut przyczyniła się do skokowego wzrostu poziomu ubankowienia – odsetek obywateli korzystających z kont bankowych wzrósł z 30% do 70%! Korzystanie z systemu finansowego to szansa na rozwój osobisty i biznesowy, co w konsekwencji prowadzi do eliminowania ubóstwa.

Podsumowując: waluty CBDC to cyfrowe wcielenie państwowego pieniądza fiducjarnego. Jest on pod całkowitą kontrolą państwa i nie

podlega takim samym mechanizmom rynkowym co zwykłe kryptowaluty. Dzięki pełnej kontroli nad CBDC państwo może arbitralnie podejść do kwestii anonimowości i polityki monetarnej; może też „programować" właściwości swojej waluty (na przykład ustalać okres ważności wypłacanych tokenów). Uważa się, że CBDC uprości i usprawni sektor finansowy. Bank Rozrachunków Międzynarodowych jest zdania, że cyfrowa waluta państwowa już opuściła domenę analiz teoretycznych i wkroczyła w fazę praktycznego eksperymentu. I taki eksperyment jest niezbędny, zanim CBDC stanie się oficjalnym cyfrowym pieniądzem przyszłości – musimy przecież ocenić, jak państwowa kryptowaluta wpływa na stabilność systemów finansowych i gospodarek.

Osobiście uważam, że blockchain jako podstawa kolejnej generacji systemów bankowych to dość naturalny i pożądany etap ich ewolucji. Warto podkreślić, że państwowy pieniądz cyfrowy to znacznie szersza idea niż kryptowaluta, i o większym potencjale niż ona. Oczywiście jestem za tym, by uważnie się przyglądać wszelkim pomysłom banków centralnych, ale przy całej tej ostrożności nie rozumiem obaw o wykorzystanie blockchaina jako silnika walut CBDC – przecież jest on (jedyną) nadzieją na jakąkolwiek transparentność finansów państwa, gdyż zapewnia możliwość obywatelskiej kontroli ich działania.

Facebook

Ostatnimi czasy w mediach głównego nurtu zrobiło się głośno o kryptowalucie Facebooka zwanej początkowo libra, a następnie diem. Projekt ten można uznać za niewypał. Dlaczego?

Facebook chciał, by przesłanie komuś pieniędzy stało się proste jak przesłanie zdjęcia. To wspaniała wizja. Projekt opierał się na powołaniu konsorcjum walidatorów. W jego skład miały wejść największe firmy technologiczne, łącznie z tymi z branży FinTech (*Financial Technology*), takimi jak Visa czy PayPal. Odpowiadałyby one za walidację transakcji dokonywanych za pośrednictwem wewnętrznej i stabilnej waluty. System miał być bardzo szybki i całkowicie ekologiczny.

Co w takim razie poszło nie tak? Od samego początku prac nad projektem Facebook zmagał się z problemami natury politycznej – zarząd Facebooka już od pewnego czasu był przesłuchiwany w związku z manipulacją danymi i nadużywaniem prywatności użytkowników. Firmie zarzucano wpływanie na wynik wyborów (wybory prezydenckie w USA i zwycięstwo Trumpa, referendum w sprawie brexitu i zwycięstwo eurosceptyków) przy wykorzystaniu zgromadzonych na platformie społecznościowej danych osobowych – na pewno słyszałeś o aferze Cambridge Analytica (znów polecę zatrważającą książkę *Mindf*ck* Christophera Wyliego).

Mimo że libra była oddzielnym bytem (stało za nią konsorcjum bardzo poważanych firm), waluta owa nie mogła się odciąć w pełni od Facebooka. Politycy i regulatorzy zadawali pytanie: „Czy chcielibyśmy powierzyć ekonomię firmie o tak wątpliwej reputacji?”.

Faktem jest, że gdyby libra była ściśle związana z Facebookiem i innymi sieciami społecznościowymi, rzeczywiście mogłaby stworzyć wielką autonomiczną ekonomię, co z kolei dałoby szerokie pole do nadużyć – w świecie wirtualnym nie istnieją poważne instytucje, które chroniłyby prawa obywatelskie. Pożyczki, kredyty i instrumenty finansowe, szybko pojawiające się na cyfrowym firmamencie Facebooka, mogłyby narazić na straty rzesze użytkowników.

Projekt powoli przygasał. Nie przeprowadzono żadnych śledztw, nie padły żadne oficjalne zarzuty, a mimo to librę, a później diem, spowiła gęsta atmosfera niesławy. Konsorcjum powoli się kurczy. Libra stała się niechcianym dzieckiem. Krążą plotki o wystawieniu jej na sprzedaż – miałaby trafić do jednego z potentatów branży IT/FinTech. Czekamy zatem na jej nowy świt…

18

Inwestycje

– Rozmawiałem ostatnio z Karolem. Podobno nieźle się dorobił na kryptowalutach… Może i my powinniśmy kupić za oszczędności trochę pieniądza elektronicznego?

– Z tego, co wiem, Karol już bardzo dawno temu kupił trochę bitcoina i czekał… Ale kiedy on kupował kryptowaluty, mało kto rozumiał, z czym to się je. A Karol zawsze był do przodu z technologią.

– To znaczy, że teraz już nie warto zaprzątać tym sobie głowy?

– No… to nie tak. Na pewno teraz jest trudniej i chyba nie ma co liczyć na jakieś duże zarobki z samych transakcji kupna-sprzedaży kryptowalut. Słyszałam za to, że warto zainteresować się spółkami, które pozyskują fundusze w blockchainie, ale nie za bardzo wiem, na czym to polega i jak w to wejść. Podobno bardziej się to opłaca…

– Hm, ja też nie wiem, o co w tym chodzi. Pogadajmy z Karolem, on na pewno rozjaśni nam w głowach.

Od zera do kryptomilionera

Pewnie nieraz słyszałeś, że ktoś zainwestował w kryptowaluty grosze, a teraz jest milionerem. Takie opowieści rozpalają wyobraźnię wizją szybkiego i łatwego zysku przy minimalnym nakładzie finansowym. No

cóż, nie będę uprzedzał faktów. W tym rozdziale przeczytasz, na czym polega inwestowanie w kryptowaluty. Przekonasz się, że nie chodzi o ich kupowanie, gdy kurs jest niski, i sprzedawanie, gdy wartość waluty rośnie. To coś o wiele bardziej złożonego i nie mniej ryzykownego. Zapraszam do lektury!

TradFi

W tradycyjnym świecie finansowym, nazywanym przez entuzjastów rozwiązań kryptowalutowych TradFi (*Traditional Finance*), mamy pełen przegląd instrumentów inwestycyjnych. Akcje, obligacje, fundusze, surowce, nieruchomości. To tylko przykłady, lista praktycznie nie ma końca i szybko przybiera dość złożoną postać. Zamiast w surowce, możemy inwestować w fundusze surowcowe. Zamiast w akcje, możemy inwestować w kontrakty wyrażające ich hipotetyczną zmianę ceny. Zamiast w konkretne nieruchomości, możemy inwestować w udziały w firmach deweloperskich. To jest płynny ekosystem zależności. Obligacje są zaciąganym długiem, który finansuje działanie państw i korporacji. Akcje wyrażają często powszechne przekonanie o reputacji przedsiębiorstw i ich wydajności.

Gotówka

DeFi (*Decentralized Finance*) to świat rynku kapitałowego działający w blockchainie. Jego rozwój rozpoczął się od pracy naukowej Satoshiego Nakamoto i od pieniądza elektronicznego. Pieniądz nie jest jednak najistotniejszym komponentem świata DeFi.

W świecie TradFi ilość pieniądza transakcyjnego (takiego, którego od razu można użyć do transakcji, czyli pieniądza o najwyższej płynności) na rynku określa się mianem agregatu M1. Nie przejmuj się – wymieniam tę nazwę tylko po to, żeby jeszcze raz unaocznić różnicę między światem zdecentralizowanym a scentralizowanym. Agregat M1 wchodzi w skład agregatu M3, który oznacza najszerzej pojęty pieniądz (również ten pod postacią oszczędności z umownym okresem wypowiedzenia, papierów wartościowych i innych aktywów, których nie można od ręki zamienić na pieniądz transakcyjny) regulowany przez bank centralny, podlegający jego arbitralnym decyzjom. Te zaś są rezultatem polityki monetarnej danego kraju.

W ostatnich latach mieliśmy okazję doświadczyć aktywności banków centralnych w tym aspekcie: dotknęły nas (co najmniej) dwa kryzysy: kryzys rynku nieruchomości w 2008 roku i kryzys pandemiczny w 2020 roku. W obydwu przypadkach polityka monetarna stała się podstawowym narzędziem walki z ich skutkami.

Polityka monetarna nie musi być złym zjawiskiem – wbrew temu, jakie wrażenie można odnieść po przeczytaniu i obejrzeniu rozmaitych materiałów w popularnych internetowych portalach. Jest raczej potwierdzeniem tezy, którą chcę tu przemycić: że pieniądz to technologia. W rozwiniętych gospodarkach zwiększenie podaży pieniądza – czyli zwiększenie jego ilości w systemie – wpłynie na rynek międzybankowy i pobudzi gospodarkę. W rozwijających się krajach to samo działanie bywa często realizacją populistycznej polityki rządu i słusznie jest nazywana drukowaniem pieniędzy.

Użytkownicy kryptowalut są wolni od rozterek związanych z podażą pieniądza, którą w zwykłej ekonomii charakteryzują wspomniane wyżej agregaty, zależne od decyzji banku centralnego. Ilość pieniądza

elektronicznego w systemie kryptowalutowym i sposób „wytwarzania” go są określone przez protokół. W przypadku bitcoina jest to formuła matematyczna, na podstawie której wylicza się, ile monet dostaną górnicy za stabilizację sieci podczas wykopywania każdego bloku. A zatem podaż bitcoina to niejako efekt uboczny poprawnej pracy jego blockchaina. Podkreślam, jest to zasada działania bitcoina – inne waluty określają swoje zasady niezależnie; panuje tu pełna dowolność i nie jest tak, że te zasady są zawsze korzystne dla danego systemu kryptowalutowego.

Warto w tym miejscu przypomnieć, że liczba monet przyznawanych górnikom zmniejsza się każdego roku o połowę. Od początku istnienia bitcoina do 2022 roku wykopano 19 z 21 milionów monet, które da się wydobyć dzięki formule matematycznej tej kryptowaluty. I mimo że nowe monety w systemie de facto generują inflację, bitcoin uważany jest za walutę deflacyjną. Nie pojawi się tu żaden bank centralny z pomysłem dosypania znikąd miliona nowych monet. Bitcoinem rządzi zdecentralizowana, dostępna dla każdego formuła, którą każdy niezależnie może zaprząc do obliczeń. Teraz chyba o wiele lepiej trafia do ciebie porównywanie bitcoina do złota: jego ilość jest skończona i z roku na rok wydobywamy go coraz mniej. Bitcoin to cyfrowe złoto.

Na zakończenie rozważań o gotówce dodam jeszcze, że inne blockchainy nie mają aż tak restrykcyjnego podejścia do inflacji jak bitcoin. Wciąż poszukuje się dobrych rozwiązań elektronicznej polityki monetarnej i inwestuje w badania nad nimi. Zdarza się wręcz często, że rozmaite systemy kryptowalutowe sztucznie ustalają bardzo wysoką inflację u swoich początków, by przyciągnąć nowych użytkowników tanim pieniądzem.

Jak widać, istnieją różne podejścia do tego tematu. Jedyną zasadą, której broniłbym niezależenie od polityki monetarnej kryptowaluty, jest

decentralizacja. Jeśli blockchain, który ci się spodobał, może dowolnie regulować ilość pieniądza w systemie, na przykład za pomocą kluczy jego założycieli, to nie ma on wiele wspólnego z decentralizacją i należy zachować ostrożność przed przystąpieniem do inwestycji.

Akcje

To właśnie między innymi dzięki akcjom tematyka kryptowalut przebiła się w końcu do szerszej świadomości.

Po co istnieją akcje? Akcje to mechanizm dostarczania pieniędzy spółkom założonym jako spółki akcyjne. Zarząd spółki sprzedaje akcje na giełdzie, a pozyskane w ten sposób fundusze trafiają na konto tej spółki. Dzięki nim może ona prowadzić swoją działalność: wybudować nową fabrykę lub zakupić maszyny. Akcje to nic innego, jak sposób finansowania przedsięwzięć.

Dzięki smartkontraktom realizacja spółki akcyjnej w blockchainie jest trywialna. Kontrakt określa liczbę specjalnych monet – tokenów – czyli akcji, i wymienia je na inne monety. Najpopularniejszym kontraktem jest ERC-20 w sieci Ethereum.

Mieliśmy okazję dyskutować to dokładniej, omawiając start-upowy serwis filmowy. Przypomnę tylko, że ów start-up zaczynał od zera, bez założycielskiego wkładu: stworzył kontrakt ERC-20 dla swojej monety (nazwijmy ją filmcoinem) i ustalił liczbę tych monet na – powiedzmy – milion. Jeśli każdą z nich sprzeda za złotówkę, zbierze milion złotych na rozwój przedsięwzięcia. Dodatkowym bonusem jest to, że gdy serwis w końcu zacznie działać, za jego usługi będzie się płaciło w filmcoinach.

Jeśli tylko cały pomysł wypali, wartość filmcoina osiągnie pożądany poziom i będzie rosła wraz ze wzrostem popytu na usługi serwisu.

Innym przykładem jest omawiany wcześniej podział na mniejsze części jakiegoś dużego i cennego dobra, takiego jak mieszkanie, biurowiec czy zabytkowy samochód. Taki podział i przyznanie współwłaścicielom stosownej puli części to przecież nic innego, jak kontrakt spółki akcyjnej w blockchainie – kontrakt tokenizujący rzeczone dobro.

ICO ze start-upami?

W świecie tradycyjnych finansów pierwsze udostępnienie akcji spółki potencjalnym nabywcom to tak zwana pierwsza oferta publiczna (*Initial Public Offering*, IPO), czyli pierwsza emisja akcji na publicznej giełdzie. Każdy może zostać współwłaścicielem spółki, kupując jej akcje. Żeby zapobiec jakimkolwiek nadużyciom, w szczególności w stosunku do niezbyt biegłych w meandrach ekonomii kontrahentów, publiczne spółki akcyjne są obwarowane gigantyczną ilością formalnych dokumentów dotyczących ich działalności i wyników finansowych. Między innymi dlatego notowanie spółki na głównych światowych giełdach nadaje jej bardzo prestiżowy status.

W świecie blockchaina też istnieje ekwiwalent IPO – ICO (*Initial Coin Offering*, co w wolnym tłumaczeniu oznacza pierwszą ofertę monet lub tokenów). Tak na marginesie wspomnę tylko, że to właśnie fala ICO z lat 2017–2019 przyczyniła się do skokowego wzrostu popularności kryptowalut i ich przebicia się do masowej świadomości. Był to czas wielkich projektów, ale też wielkich oszustw. Niesamowite wahania cen

kryptowalut stworzyły nie tylko nowych milionerów, ale także były powodem wielu dramatycznych bankructw.

ICO działa w blockchainie, więc ze względu na swój stuprocentowo cyfrowy charakter jest bardzo dobrym sposobem pozyskiwania finansów na nowe „cyfrowe przedsięwzięcia". Przykład z serwisem filmowym pokazał, że można w ten sposób stworzyć cały domknięty ekosystem. W blockchainie nie istnieje żadna centralna instytucja – nie ma tam zatem żadnego uprawnionego organu, który mógłby sprawdzić kondycję finansową i wiarygodność firmy oferującej swoje udziały oraz obiecującej spożytkować pozyskane z ICO środki na swój rozruch i rozwój. Inwestowanie w takie spółki jest więc niesamowicie ryzykowne. Szczerze mówiąc, uważam, że to najbardziej ryzykowna forma inwestowania, jaką znam.

ICO jest zarazem najbardziej elastyczną formą pozyskiwania funduszy przez założycieli firm i start-upów. Pozwala budować ekonomię wokół swojego produktu i monitorować popularność choćby aplikacji. Przez relatywną łatwość i bezkosztowość procesu emisji monet pozwala szerszej publice uczestniczyć w bardzo wczesnych etapach powstawania start-upu. Z tego wynika, że da się tu zarobić najwięcej w stosunku do zainwestowanego wkładu – pod warunkiem, że firma się rozwinie i odniesie sukces.

Po roku 2019 rynek ICO znacznie się schłodził, ale gdy przeżywał swoją koniunkturę, mechanizm ICO pozyskał na inwestycje ponad dwadzieścia miliardów dolarów! Wiele ze sfinansowanych wówczas projektów do dziś gości w zestawieniu dwustu najbogatszych pod względem kapitalizacji firm w blockchainie. Z ICO sfinansowano też rozmaite badania kryptograficzne i informatyczne, które wydatnie przesunęły granice możliwości cyfrowego świata.

Nie obyło się też bez matactw, jednak doniesienia prasowe, jakoby 99% spółek oferujących ICO było oszustami, to coś, co jest wręcz fizycznie niemożliwe. Takich ewidentnych przekrętów zdarzyło się kilkanaście, może kilkadziesiąt, a ich początkowa wycena wynosiła kilka milionów dolarów. Jednymi z lepszych dowcipnisiów (choć inwestorzy inaczej by ich nazwali) okazali się założyciele start-upu, który dzień po zebraniu funduszy zastąpił zawartość swojej pięknej strony internetowej pojedynczym słowem: „penis”.

Żeby uniknąć oszustw na większą skalą, rynek ICO analizuje pierwsze oferty monet, gdy ich wartość przekracza 50 milionów dolarów. Przy takich sumach wymaga się od firm przejrzystej dokumentacji zarówno oferty, jak i samego przedsiębiorstwa. Z analizy rynku dość jednoznacznie wynika, że w przypadku około 80% projektów ICO nie udało się utrzymać płynności w cenie dorównującej początkowej ofercie. Zatem około 80% projektów po prostu upadło, nie zyskało spodziewanej popularności lub wręcz w ogóle nie powstało.

Czy jednak możemy taki stan rzeczy nazwać oszustwem? W Dolinie Krzemowej – kolebce start-upów technologicznych – kapitał zapewniają fundusze Venture Capital – to one obserwują firmy od ich najwcześniejszych chwil, nawet od momentu powstania wizji produktu. Trudno zdobyć jakiekolwiek wiarygodne statystyki, ale tajemnicą poliszynela jest, że fundusze VC inwestują w jeden na czterysta start-upów ubiegających się o środki. I tylko jedno z dziesięciu dofinansowanych w ten sposób przedsiębiorstw przynosi następnie jakiekolwiek zyski. I tylko co czwarty z funduszy VC inwestuje lepiej niż szeroki rynek.

Skuteczność ICO na tym tle wypada całkiem nieźle. Biorąc pod uwagę, że fundusze VC z całą swoją wiedzą o strukturze i planach przedsiębiorstw potrafią wyłuskać tylko jednego spośród czterech tysięcy kandydatów…

Zauważ, jakie to nieprawdopodobnie trudne zadanie: przeprowadzić udaną inwestycję.

Branża informatyczna, a w szczególności branża start-upów technologicznych, jest jedną z najbardziej ryzykownych pod względem inwestycyjnym.

Inwestować czy nie?

Być może lekturę tego rozdziału rozpoczynałeś z nadzieją, że dowiesz się, jak inwestować w kryptowaluty. Czy warto to robić? Czy nie inwestując, przegapiasz jakąś dziejową okazję na pomnożenie majątku?

Mam nadzieję, że teraz już dostrzegasz, jakie to trudne. Inwestorzy kryptowalutowi mają bardzo pod górkę.

No dobrze. Wciąż jesteś zainteresowany inwestycją w kryptowaluty? Widzę zatem kilka możliwości. Tylko proszę, nie traktuj ich jako wiążących porad inwestycyjnych.

Po pierwsze, gdy szukamy ryzykownej inwestycji o dużym potencjale wzrostu i zakładamy, że możemy stracić do 5% środków z naszego portfela oszczędności, to kryptowaluty z listy stu najlepszych pod względem kapitalizacji sprawdzą się jak żaden inny instrument finansowy. Na pewno nie zawiodą pod względem wahań cen i dostarczania emocji!

Po drugie, wejście w świat kryptowalut otwiera wiele drzwi: poznamy zespoły budujące nowe blockchainy i oparte na nich produkty. Taka wiedza pomoże ocenić wartość użytkową obserwowanego start-upu i zmniejszy ryzyko inwestycji.

Po trzecie, musimy pamiętać, że nawet jeśli pozytywnie ocenimy ten czy inny start-up, ryzyko wciąż będzie spore. Nawet najbardziej

przełomowe pomysły i niezwykle obiecujące koncepcje mogą z różnych powodów nie wypalić. Inwestuj w wybrany temat swój czas, powiększaj wiedzę i umiejętności, ale oszczędności ulokuj bezpiecznie gdzie indziej. Być może wraz z rozwojem projektu, który tak ci się spodobał, uznasz, że warto wesprzeć daną inicjatywę – mimo ryzyka utraty części oszczędności. Pamiętaj jednak, że najlepszą inwestycją będzie twoja edukacja.

Inną możliwość stwarzają działające w blockchainie platformy crowdfundingowe. To chyba najlepsze rozwiązanie dla początkujących inwestorów – uznane firmy z branży finansowania społecznościowego zawsze wstępnie sprawdzają wiarygodność start-upów ubiegających się o środki, a blockchain daje nam możliwość audytu parametrów akcji i przebiegu zbiórki. Trzeba jednak pamiętać, że crowdfunding nie jest prawdziwą inwestycją – to dobre narzędzie wspierania ciekawych inicjatyw i koncepcji produktów. Raczej nie ma tu mowy o udziałach w danej firmie. Często jedyną nagrodą za sukces zbiórki i rozkręcenie start-upu jest jego produkt – wysyłany do wspierających jeszcze przed oficjalnym rynkowym debiutem. Przez udział w crowdfundingowych zbiórkach lepiej też poznamy cały ekosystem.

We wszystkich przypadkach trzeba mieć zawsze świadomość faktu, że profesjonalne fundusze inwestycyjne z całą swoją wiedzą i doświadczeniem dokonują udanej inwestycji raz na kilka tysięcy przypadków. Wciąż jestem zdania, że najlepszą inwestycją jest poświęcenie czasu na edukację o nowym świecie inwestycji i finansów. Być może nowo nabyta wiedza sprzedana funduszom inwestycyjnym przyniesie więcej zysku niż bezpośrednie inwestycje w tokeny?

19

Krótkie kompendium

Powoli zbliżamy się do końca naszej wspólnej podróży po świecie kryptowalut, blockchainów, smartkontraktów, Dowodów Pracy i Udziału… Mam nadzieję, że ci się podobało. Starałem się, by ta książka nie była nudnym wykładem – zależało mi na wspólnym odkrywaniu nowych obszarów i zaglądaniu w ciekawe miejsca, w tym „pod maskę” kryptowalutowych „silników”. Chciałem ci pokazać, że kryptowaluty to nie tylko nowa forma pieniędzy, ale przede wszystkim technologiczna innowacja o kapitalnym znaczeniu dla naszego rozwoju cywilizacyjnego.

Napisałem tę książkę w formie lekkiej opowieści, luźnej i nie za długiej gawędy dla zabieganych. Wyjaśnienia, jak działają kryptowaluty i blockchain, przeplatałem przykładami, ciekawostkami oraz opisami rzeczywistych i hipotetycznych sytuacji, w których kryptowaluty i blockchain pokazują swój potencjał.

Myślę, że dobrym pomysłem będzie zebranie wszystkich podstawowych informacji o kryptowalutach w jednym miejscu, w bardzo skondensowanej formie. Czytając poniższą listę, z łatwością przypomnisz sobie wszystkie konteksty, w których pojawiały się poszczególne definicje i wyjaśnienia, i utrwalisz swoją wiedzę. Pojawi się też trochę nowości – być

może część z nich to rzeczy, o które chciałeś zapytać podczas lektury poprzednich rozdziałów, zaś przy pomocy pozostałych z łatwością uzupełnisz swój zasób kryptowalutowych informacji. Mam tu na myśli szczególnie ostatnie punkty listy, gdzie piszę o pożyczkach i innych instrumentach finansowych, które ujawniają możliwości świata zdecentralizowanych finansów (DeFi).

1. Co to jest blockchain?

Blockchain to bardzo specyficzna baza danych, platforma, która umożliwia działanie kryptowalut. Blockchain działa jak księga rachunkowa – zapisuje wszystkie transakcje, ale nie chodzi tu wyłącznie o transakcje pieniężne. Blockchain zapamiętuje na zawsze wszelkie zmiany, które są w nim zapisywane, dzięki czemu ma funkcję audytu operacji. Wbudowany w każdy blockchain mechanizm monet (tokenów) nadaje mu płynność transakcyjną. Blockchain może być publiczny (choć nie musi).

2. Czym jest kryptowaluta? Ile jest kryptowalut i blockchainów?

Kryptowaluta to pieniądz elektroniczny, ale z technicznego punktu widzenia można ją rozumieć jako aplikację działającą w blockchainie. W jednym blockchainie może działać wiele różnych kryptowalut. Istnieje wiele sieci utrzymujących rozmaite blockchainy. Obecnie są ich dziesiątki tysięcy.

3. Co to jest smartkontrakt?

Smartkontrakt, zwany także inteligentnym kontraktem, to program zawierający umowę. W tej umowie ustalamy, co ma się dziać ze środkami, którymi zarządza smartkontrakt. Kiedy umieścimy smartkontrakt

w blockchainie, zacznie on wykonywać zapisy naszej umowy całkowicie automatycznie.

4. Czym są tokeny kryptowalutowe?

Tokeny, inaczej monety, to jednostki kryptowaluty działającej w blockchainie. Mogą nimi być monety powołane do życia w jakimś smartkontrakcie jednego blockchaina. Mogą to być natywne monety różnych blockchainów. Tokeny można rozumieć jak nośniki – krwinki w krwiobiegu kryptowaluty.

5. Czy każdy blockchain umożliwia działanie smartkontraktów?

Nie. Niektóre blockchainy skupiają się wyłącznie na obsłudze transferu tokenów, czyli monet. Tak przykładowo działa Bitcoin. Pierwszym blockchainem, który otworzył się dla smartkontraktów, jest Ethereum. Przychodzi mi do głowy pewna – może nieco łopatologiczna – analogia: w bardzo dużym uproszczeniu różnica między smartkontraktowym a czysto kryptowalutowym blockchainem jest mniej więcej taka, jak różnica między klasycznym telefonem z kablem a smartfonem. Telefony z kablem są niezawodne, ale ograniczone tylko do jednej funkcji: rozmowy telefonicznej. Smartfon ma multum rozmaitych funkcji i daje nieograniczone możliwości, ale… czasem lubi się zawiesić.

6. Jak wygląda smartkontrakt?

Oto przykładowy smartkontrakt do wypłacania kieszonkowego twoim dzieciom. Nawiasy okrągłe zawierają zmienne: (komu_wypłacić) – to adresy portfeli dzieci, (ile) – wysokość kieszonkowego, a w nawiasach kwadratowych – instrukcje do wykonania:

[KOMU WYPŁACIĆ (komu_wypłacić)]
[ILE (ile)]

[SPRAWDŹ ŚRODKI]

[SPRAWDŹ DATĘ]

[JEŚLI jest pierwszy dzień miesiąca ORAZ istnieją środki w kontrakcie PRZEKAŻ (komu_wypłacić) (ile)]

Z czym ci się to kojarzy? Pewnie ze zleceniem automatycznego przelewu cyklicznego w banku. To też bardzo dobry przykład smartkontraktu (tyle że działa w banku, a nie w blockchainie). Rzecz jasna, smartkontrakty z reguły bywają o wiele bardziej złożone niż nasze przykłady.

7. Co to jest gaz (zwany czasem paliwem) smartkontraktu?

Gaz smartkontraktu to dodatkowe środki kryptowalutowe, które są potrzebne, żeby zrealizować ustalenia umowy. W blockchainie nie ma nic za darmo. Jeśli chcę przelać środki, to po pierwsze – muszę je mieć, a po drugie – muszę zapłacić za ich transfer. Realizacja smartkontraktu to wiele mikrooperacji, czyli mikroobliczeń blockchaina – gaz zużywamy właśnie na ich przeprowadzanie. Pamiętaj: energia kosztuje.

8. Czy smartkontrakt działa jak zwyczajna internetowa aplikacja?

Tak, smartkontrakt działa podobnie, ma jednak wiele dodatkowych cech.

Pierwszą z nich jest to, że zasady działania smartkontraktu mogą być sprawdzone przez użytkowników (w blockchainach, które są publiczne). Drugą z kluczowych cech smartkontraktów jest zachowywanie historii

wszystkich operacji i interakcji między użytkownikami blockchaina. Trzecią wyróżniającą smartkontrakty cechą (i zaletą) jest gwarancja nienaruszalności umowy. Autor aplikacji opartej na smartkontrakcie nie może złamać z góry ustalonych zasad. Jeśli smartkontrakt sprzedaje w grze magiczne miecze, a jego autor zadeklarował, że jest ich tylko pięć i że nie można zmienić tej liczby, to mamy gwarancję, że w ramach tego konkretnego smartkontraktu nigdy nie powstaną dodatkowe miecze. Przy okazji: ten kontrakt z mieczami to oczywiście… kontrakt NFT!

9. Jak zacząć używać blockchaina?

Trzeba najpierw stworzyć własną tożsamość za pomocą tak zwanego portfela. „Pod maską” portfeli blockchainowych działają zaawansowane, nowoczesne narzędzia kryptograficzne. Portfele generują klucze publiczne, których używamy, by się przedstawiać innym użytkownikom blockchaina i otrzymywać od nich środki, oraz klucze prywatne, które pełnią funkcję hasła (od zwykłych haseł są jednak o wiele dłuższe – to kilkustronicowe ciągi znaków). Klucze prywatne odblokowują nasze środki i pozwalają je transferować na inne konta (adresowane kluczami publicznymi ich użytkowników). Klucze prywatne są naszą tajemnicą, gdyż strzegą naszych środków. Nie możemy ich nikomu przekazywać! Są tak ważne, że jeśli nasze transakcje opiewają na większe sumy, najlepiej stosować ich sprzętową ochronę: istnieją specjalne urządzenia przypominające pendrive’y, które zapewniają ich bezpieczne przechowywanie. Nazywa się je się portfelami sprzętowymi. Dwóch najbardziej znanych producentów tych urządzeń to Ledger i Trezor.

10. Jak działać z NFT?

Na wiodących portalach aukcyjnych NFT można znaleźć instrukcję, jak uruchomić własny kontrakt, który będzie rozpoznany przez dany serwis. Kiedy już nasz smartkontrakt zacznie działać, inni użytkownicy będą mogli przeglądać i licytować jego tokeny (monety), reprezentujące nasze utwory, grafiki, certyfikaty – słowem: wszystkie posiadane przez nas NFT, którymi chcemy handlować. Kiedy ktoś je kupi, nabyty NFT zostanie przypisany do kupującego. Kupujący jest zwykle identyfikowany przez swój klucz publiczny. Aby sprzedać NFT, potrzebujemy swojego klucza prywatnego.

11. Gdy dostanę przelew na konto, chcę wymienić otrzymaną kryptowalutę na inną – jak to zrobić?

Chcąc dokonać wymiany, musimy użyć giełdy walutowej. Istnieją oficjalne giełdy, które są legalnie działającymi firmami. Musimy mieć w ich systemie swoje konto. Tam przelewamy środki i w obrębie giełdy wymieniamy je na inną walutę. Wadą tego rozwiązania jest powierzenie giełdzie własnych środków na czas ich wymiany. Alternatywne rozwiązanie stanowią giełdy zdecentralizowane, które są smartkontraktami. Odnajdujemy jedną z nich, na przykład Uniswap – ważne, by obsługiwała potrzebną nam parę walutową. Deponujemy nasze środki w wejściowej walucie pary i odbieramy je przeliczone na walutę wyjściową.

12. Czy mogę w blockchainie otrzymać pożyczkę?

Tak! Zwykle pożyczek po wpłaceniu zastawu udzielają smartkontrakty. Z pożyczek korzystamy po to, by mieć dostęp do innej kryptowaluty bez pozbywania się tej, którą posiadamy. Jednym z powodów zaciągania pożyczki jest choćby nasze przekonanie, że kurs zastawianej kryptowaluty może w przyszłości być wyższy – dlatego nie chcemy się jej pozbywać. A dzięki pożyczce przez jakiś czas mamy do dyspozycji inną, potrzebną

nam w danej chwili walutę. Zastawy bywają dość wysokie – zwykle możemy pożyczyć około połowę zastawionej kwoty.

13. Czy mogę zarabiać na udzielaniu pożyczek?

Tak! Drugim aspektem kontraktów pożyczkowych jest możliwość deponowania środków, które są oprocentowane niżej niż pożyczki. W blockchainie stopy procentowe oblicza się w czasie rzeczywistym – są wynikiem działania matematycznego, a nie deklaracji urzędów.

14. Jak zmienić pożyczkę na korzystniejszą w innym kontrakcie?

Gdy zauważymy korzystniejszą ofertę pożyczki, możemy niemal bezkosztowo zmienić dostawcę tej dotychczasowej. W tym celu korzystamy z tak zwanych pożyczek błyskawicznych (*flash loans*). Możemy w jednej transakcji otrzymać pożyczkę błyskawiczną, spłacić bieżący dług, odzyskać zastaw, wpłacić zastaw w innym kontrakcie i nową pożyczką spłacić pożyczkę błyskawiczną! Łączenie pożyczek i zastawów w takie łańcuchy zależności pozwala na stworzenie skomplikowanych instrumentów finansowych, jak syntetyczne papiery wartościowe, kontrakty różnicy kursowej i tym podobne.

15. Jakie inne smartkontrakty finansowe są dostępne w kryptowalutowym świecie zdecentralizowanych finansów, czyli DeFi?

Wyliczam (oczywiście to tylko przykłady): kontrakty stablecoin, czyli monet stabilnych, które utrzymują wartość monety na poziomie waluty fiducjarnej, choćby dolara (pamiętasz o MakerDao?); odpowiedniki funduszy indeksowych ETF o określonych aktywach (Balancer); kontrakty depozytowe i pożyczkowe ze stałą i zmienną stopą procentową (Yield,

Compound, Aave, dYdX); kontrakty z lewarowaną pozycją; kontrakty ubezpieczeniowe, które wypłacają środki w określonych umową przypadkach; i wiele, wiele innych.

16. W jaki sposób kontrakty ubezpieczeniowe lub kontrakty stabilne „dowiadują się" o cenach i wydarzeniach ze świata rzeczywistego?

Istnieje specjalne narzędzie przekazujące dane do blockchaina – nazywa się wyrocznią. Zapisuje ono dowolne potwierdzone dane, takie jak pożary budynków, powodzie, ale też aktualny kurs bitcoina w dolarach.

17. Czy kryptowaluty chronią przed inflacją?

Nic na to nie wskazuje. Pomimo deflacyjnego charakteru protokołów takich jak Bitcoin, historia kursu bitcoina do dolara nie przejawiała charakteru przeciwinflacyjnego. Kryptowaluty są postrzegane jako ryzykowne instrumenty finansowe, a ich kurs wydaje się korelować z cenami akcji firm technologicznych.

18. Jakie są ryzyka operacji finansowych w blockchainie?

Tu też wyliczam, starając się tym razem wspomnieć o wszystkich czyhających na nas zagrożeniach, bo to bardzo ważne: utrata dostępu do portfela, kradzież kluczy prywatnych, błąd użytkownika przy korzystaniu z portfela, nadużycia niskopoziomowych (czyli zaawansowanych, odpowiedzialnych za kodowanie) użytkowników sieci, błędy w smartkontraktach, które są wykorzystywane przez nieuczciwych użytkowników, błędy w skomplikowanych scenariuszach zależności między smartkontraktami, nowe prawodawstwo regulujące w nieprzewidziany sposób obrót kryptowalutami, wahania cen kryptowalut

podstawowych i pochodnych. Słowem: musisz uważać, ale wiedza i ostrożność powinny cię uchronić od wpadki. W internecie oszustwa zdarzają się wszędzie, ale kiedy ma się głowę na karku, można się przed nimi ustrzec. Zasada ograniczonego zaufania nie obowiązuje wyłącznie na drodze.

Zakończenie

Żyjemy w świecie, w którym ludzie sobie nie ufają. I słusznie. Czy kiedyś było inaczej, lepiej? Pewnie nie. Dziś jednak mamy technologię, dzięki której możemy dokonać przełomu w tej dziedzinie.

Blockchain.

Czy dzięki niemu zaczniemy sobie ufać? I tak, i nie – to bez znaczenia. Celem blockchaina jest stworzenie platformy zaufania, która pozwoli nam współpracować… bez zaufania. To coś zupełnie nowego.

Musimy jednak koniecznie zmienić postrzeganie kryptowalut – uwolnić się od myślenia o nich jako instrumencie spekulacji i przesunąć środek ciężkości kryptowalutowej debaty ku blockchainowi.

Blockchain to nowa jakość w historii ludzkości.

Potrzebujemy tej nowej jakości.

Świat bardzo się zmienił, odkąd pojawił się internet. Zmalały odległości. Rozmyły się granice między społecznościami. Dochody korporacji technologicznych przewyższyły budżety narodowe niektórych państw. Co więcej, firmy te są zorganizowane i zarządzane lepiej niż większość krajów.

Sieci społecznościowe nadwerężyły demokrację, spolaryzowały i rozjątrzyły debatę publiczną, a także podważyły zaufanie do ekspertów.

Nowoczesne banki i firmy z branży finansowej umożliwiają nam sprawne zarządzanie własnymi pieniędzmi, ale jesteśmy na ich łasce. One zaś są na łasce inwestorów i rządów.

Prywatność i poufność praktycznie nie istnieją. Ani nasze prywatne wiadomości, ani codzienne użytkowanie internetu nie są wyłącznie naszą osobistą sprawą.

Czyżbyśmy się pogubili?

Wygląda na to, że nasze cudowne wynalazki zamiast służyć, zaczęły nam trochę szkodzić. Nie chcemy jednak z nich rezygnować. Oferują przecież tyle dobrego. Trudno by było bez nich żyć.

Odzyskajmy inicjatywę.

Odwróćmy kolejność technologicznego łańcucha pokarmowego. Stańmy się znowu jego ostatnim ogniwem.

Blockchain i kryptowaluty to nasza nowa nadzieja.

Już kilkadziesiąt sieci społecznościowych używa tej technologii do tworzenia wartościowych treści.

Zdecentralizowane systemy finansowe mogą już dziś zaspokoić wszelkie zróżnicowane potrzeby. Zapewnią bezpieczną przystań dla naszych oszczędności i w ułamku sekundy zrealizują przelew. Umożliwią aktywne inwestowanie. Udostępnią nam instrumenty finansowe zarezerwowane dotychczas wyłącznie dla wielkich banków inwestycyjnych.

A wszystko to bez władzy nad nami i nad naszą własnością.

Proekologiczne zachęty i optymalizacja naszego życia pod względem energooszczędności, ale bez rezygnowania z komfortu i wygody; nowe, skuteczniejsze i mniej podatne na zewnętrzne wpływy i populizm modele

demokracji; szybsze, wygodniejsze – i bezpieczniejsze – sposoby zmiany statusu własności; śledzenie łańcuchów dostaw w trosce o zdrowie i ekologię; nowy wymiar rozrywki; usprawnienie opieki medycznej… Wszystko to realizuje blockchain, który dodatkowo w swojej najnowszej odsłonie staje się kołem zamachowym czystej, bezemisyjnej przyszłości.

Budujemy most łączący dwa światy – tradycyjny i wirtualny. To skomplikowana konstrukcja, która stawia przed nami sporo wyzwań, ale i otwiera całe spektrum możliwości.

Niezależność, decentralizacja, prywatność, produktywność, wygoda, bezpieczeństwo.

Mam nieodparte wrażenie, że to właśnie blockchain stanie się kolejnym etapem ewolucji cyfrowego człowieka i że jego znaczenie dla naszego rozwoju okaże się porównywalne z przeskokiem, jaki dokonał się pośród wędrownych ludów, gdy udomowiono zwierzęta, zaczęto uprawiać ziemię i praktykować osiadły tryb życia.

Blockchain „terraformuje” dziki cyfrowy świat – tworzy w nim niszę ekologiczną, środowisko przyjazne człowiekowi. Potrzebujemy go, by wspiąć się jeszcze wyżej!

To wszystko dzieje się teraz, na naszych oczach.

Nie spóźnijmy się na ten pociąg!

Podziękowania

Podziękowania kieruję zgodnie z chronologią wydarzeń, która wprowadziła mnie na kryptowalutową ścieżkę i dała możliwość wzięcia udziału w tej niesamowitej przygodzie.

Chciałbym podziękować całemu zespołowi blockchaina Aeternity. Był to pierwszy blockchain w moim życiu, projekt, który napisaliśmy od zera i który nas ukształtował. W czasach, gdy nie było praktycznie żadnej dokumentacji ani samouczków, stawialiśmy pierwsze kroki razem, wspólnie się ucząc i przekuwając zdobytą wiedzę w kod. W szczególności dziękuję założycielowi i CEO Aeternity Yaniemu Malahovowi, który działa w branży kryptowalutowej od samego jej początku. Tocząc z nami niekończące się dyskusje o ekonomii, polityce i etyce zaszczepiłeś w nas skutecznie wiele cyberpunkowych i cypherpunkowych idei! Dzięki, to były niesamowite lata!

Pisanie blockchaina to dla architekta systemu olbrzymie wyzwanie. Niespodziewane wyjazdy, wielodniowe konferencje, koordynacja zespołów na przeciwległych krańcach kontynentu. Chciałbym podziękować mojej żonie Oli, która mnie wówczas wspierała, szczególnie gdy wiele razy z dnia

na dzień musiałem cię zostawić w domu ze wszystkimi trzema mieszkającymi w nim krasnoludkami.

Na zakończenie chciałbym podziękować całemu zespołowi wydawnictwa Insignis. W szczególności Pawłowi Brzozowskiemu, który namówił mnie na wyciągnięcie materiałów z szuflady i napisanie tej książki, oraz Tomaszowi Brzozowskiemu, który nadał jej ostateczną formę. Nie pracowaliśmy w tym samym biurze, ale nieraz czułem, jak wirtualnie marszczysz czoło, nie tylko nad szykiem moich zdań, ale też kiedy wspólnie zastanawialiśmy się nad jak najlepszą argumentacją kryptopomysłów. Dzięki!

O autorze

Michał Zajda – polski informatyk, weteran Doliny Krzemowej.

Urodził się w 1985 roku w Katowicach. Od zawsze interesowała go matematyka i nauki ścisłe. Uczeń „klasy kwadratów” VIII Liceum Ogólnokształcącego w Katowicach i bywalec pracowni matematyki i informatyki katowickiego Pałacu Młodzieży. Absolwent krakowskiej Akademii Górniczo-Hutniczej („wydział samogłosek”, kierunek: informatyka).

Karierę zawodową rozpoczął od opanowania niszowej technologii Erlang wywodzącej się ze szwedzkich laboratoriów firmy Ericsson.

Przełomowa okazała się dla niego kilkuletnia praca w Dolinie Krzemowej. W jednym z tamtejszych start-upów odpowiadał za wydajność i niezawodność systemu, który obsługiwał powiększającą się lawinowo liczbę użytkowników – ta pod jego nadzorem wzrosła od miliona do niemal trzystu milionów. To wówczas zdobył olbrzymie doświadczenie z dziedziny automatyzacji, zarządzania zespołami i tak zwanych technik zwinnych.

W ciągu kilkunastu lat zdążył pracować przy najciekawszych jego zdaniem projektach cyfrowego świata. Zajmował się przede wszystkim problematyką rozległych systemów informatycznych, takich jak

komunikatory internetowe, systemy sztucznej inteligencji i autonomicznych botów, a także sieci urządzeń internetu rzeczy. Z sukcesami mierzył się z największym wyzwaniem co do tych systemów: zapewnieniem ich niezawodności i wydolności przy zwiększającej się liczbie użytkowników. Jego szczególną uwagę zawsze zaprzątało ryzyko zagrażające rozwojowi systemów na styku przemysłu i badań. Jego doświadczenie w branży pomogło wielu start-upom z całego świata, które zderzyły się nagłą falą popularności.

Zrządzeniem losu kilka lat temu zainteresował się zupełnie nowym obszarem technik informatycznych – systemami kryptowalutowymi. Został architektem, programistą i menedżerem jednego z pierwszych blockchainów nowej generacji.

Fascynują go idee tkwiące u podstaw filozofii kryptowalut, wyrażone między innymi w pracach pierwszych twórców tej innowacyjnej technologii. Z pasją dzieli się swoją wiedzą i zainteresowani z innymi, czego wyrazem jest między innymi niniejsza książka.

Obecnie stoi na czele kameralnego zespołu informatyków w swojej własnej firmie zajmującej się pracami badawczo-rozwojowymi oraz architekturą skalowalnych systemów informatycznych. Specjalizuje się w algorytmach konsensusu w sieciach publicznych.